On Proofs of Existence by Abundance

Léonard Cadilhac

Lecteur Hadamard 2020 - 2024

September 1, 2020

Three meanings for "many"

Mainly three approaches to get an intuition of the size of a set:

Three meanings for “many”

Mainly three approaches to get an intuition of the size of a set:

- Logical (cardinality)

Three meanings for “many”

Mainly three approaches to get an intuition of the size of a set:

- Logical (cardinality)
- Topological (dense open sets, Baire’s property)

Three meanings for “many”

Mainly three approaches to get an intuition of the size of a set:

- Logical (cardinality)
- Topological (dense open sets, Baire’s property)
- Probabilistic or measure theoretic (sets of measure 1 or more generally of positive measure)

Existence using cardinality

Transcendental numbers

There exist transcendental real numbers (real numbers which are not the roots of any rational polynomial).

- **Proof**: there are countably many algebraic numbers and uncountably many real numbers.
- First example given by Liouville (1844):

$$\sum_{k=1}^{\infty} 10^{-k!}.$$

Describable numbers

Describability (loose definition)

A real number is said to be *describable* if there exists a finite mathematical proposition identifying it.

Describable numbers

Describability (loose definition)

A real number is said to be *describable* if there exists a finite mathematical proposition identifying it.

- Most real numbers are not describable!
- Algebraic numbers, π, e, $0,123456789101112\ldots$ are describable.

Baire's property

Baire's property

A countable intersection of dense open sets is dense.

Baire's property

Baire's property

A countable intersection of dense open sets is dense.

Theorem

Baire's property is true for Polish spaces (separable completely metrizable spaces).

Baire's property

Baire's property

A countable intersection of dense open sets is dense.

Theorem

Baire's property is true for Polish spaces (separable completely metrizable spaces).

- Note the useful equivalent of Baire's property: a countable union of closed sets with empty interior has empty interior,
- a property satisfied on an intersection of dense open sets is said to be **typical**.

Nowhere differentiable continuous functions

Weierstrass function (1872)

Let $b \in (0,1)$, a an odd positive integer and $ab > 1 + 3\pi/2$. The function:

$$f : x \mapsto \sum_{n=1}^{\infty} b^n \cos(a^n \pi x)$$

is continuous but nowhere differentiable on $\mathbb{R}$.

Nowhere differentiable continuous functions

Weierstrass function (1872)

Let $b \in (0,1)$, a an odd positive integer and $ab > 1 + 3\pi/2$. The function:

$$f : x \mapsto \sum_{n=1}^{\infty} b^n \cos(a^n \pi x)$$

is continuous but nowhere differentiable on $\mathbb{R}$.

The Baire method approach

Being nowhere differentiable is a *typical* property of continuous functions.

Nowhere differentiable continuous functions

Weierstrass function (1872)

Let $b \in (0,1)$, a an odd positive integer and $ab > 1 + 3\pi/2$. The function:

$$f : x \mapsto \sum_{n=1}^{\infty} b^n \cos(a^n \pi x)$$

is continuous but nowhere differentiable on $\mathbb{R}$.

The Baire method approach

Being nowhere differentiable is a *typical* property of continuous functions.

Scheme of proof

- X: continuous functions on $[0,1]$ with the usual norm,
- Define, for any $n \in \mathbb{N}$:
  $$F_n := \{f \in X : \exists x \in [0,1], \forall y \in [0,1], |f(x) - f(y)| \leq n\,|x - y|\}.$$
- F_n is closed with empty interior so $F = \bigcup_n F_n$ has empty interior.
- F contains the set of functions with at least one point of differentiability.

Conclusion so far

- Proofs by abundance are often less technical and give information about the whole space. They are however not constructive.

Conclusion so far

- Proofs by abundance are often less technical and give information about the whole space. They are however not constructive.
- Typical $\neq$ Usual!
  Typical behaviours can very well be **pathological**.

Operators on Hilbert spaces

- Let $\mathcal{H}$ be an (infinite) dimensional Hibert space and $\mathcal{B}(\mathcal{H})$ the space of bounded operators on $\mathcal{H}$.

Operators on Hilbert spaces

- Let $\mathcal{H}$ be an (infinite) dimensional Hibert space and $\mathcal{B}(\mathcal{H})$ the space of bounded operators on $\mathcal{H}$.
- $\mathcal{B}(\mathcal{H})$ can be endowed with various natural topologies such as:
  - norm topology: $\|T\|_{op} = \sup_{x\in\mathcal{H}} \frac{\|T(x)\|}{\|x\|}$.

Operators on Hilbert spaces

- Let $\mathcal{H}$ be an (infinite) dimensional Hibert space and $\mathcal{B}(\mathcal{H})$ the space of bounded operators on $\mathcal{H}$.
- $\mathcal{B}(\mathcal{H})$ can be endowed with various natural topologies such as:
  - norm topology: $\|T\|_{op} = \sup_{x\in\mathcal{H}} \frac{\|T(x)\|}{\|x\|}$.
  - strong operator topology:
  $$T_n \to T \Leftrightarrow \forall x \in \mathcal{H}, T_n(x) \to T(x),$$

Operators on Hilbert spaces

- Let $\mathcal{H}$ be an (infinite) dimensional Hibert space and $\mathcal{B}(\mathcal{H})$ the space of bounded operators on $\mathcal{H}$.
- $\mathcal{B}(\mathcal{H})$ can be endowed with various natural topologies such as:
  - norm topology: $\|T\|_{op} = \sup_{x\in\mathcal{H}} \frac{\|T(x)\|}{\|x\|}$.
  - strong operator topology:
  $$T_n \to T \Leftrightarrow \forall x \in \mathcal{H}, T_n(x) \to T(x),$$
  - strong-$\star$ operator topology:
  $$T_n \to T \Leftrightarrow \forall x \in \mathcal{H}, T_n(x) \to T(x) \text{ and } T_n^*(x) \to T^*(x).$$

Operators on Hilbert spaces

- Let $\mathcal{H}$ be an (infinite) dimensional Hibert space and $\mathcal{B}(\mathcal{H})$ the space of bounded operators on $\mathcal{H}$.
- $\mathcal{B}(\mathcal{H})$ can be endowed with various natural topologies such as:
  - norm topology: $\|T\|_{op} = \sup_{x\in\mathcal{H}} \frac{\|T(x)\|}{\|x\|}$.
  - strong operator topology:
$$T_n \to T \Leftrightarrow \forall x \in \mathcal{H}, T_n(x) \to T(x),$$
  - strong-$\star$ operator topology:
$$T_n \to T \Leftrightarrow \forall x \in \mathcal{H}, T_n(x) \to T(x) \text{ and } T_n^*(x) \to T^*(x).$$

Linear dynamics on Hilbert spaces (Grivaux, Matheron, Menet 2017)

Studying typical properties of operators with respect to these topologies, they proved the existence of operators with particular dynamical properties.

Operators on Hilbert spaces

- Let $\mathcal{H}$ be an (infinite) dimensional Hibert space and $\mathcal{B}(\mathcal{H})$ the space of bounded operators on $\mathcal{H}$.
- $\mathcal{B}(\mathcal{H})$ can be endowed with various natural topologies such as:
  - norm topology: $\|T\|_{op} = \sup_{x\in\mathcal{H}} \dfrac{\|T(x)\|}{\|x\|}$.
  - strong operator topology:
  $$T_n \to T \Leftrightarrow \forall x \in \mathcal{H}, T_n(x) \to T(x),$$
  - strong-$\star$ operator topology:
  $$T_n \to T \Leftrightarrow \forall x \in \mathcal{H}, T_n(x) \to T(x) \text{ and } T_n^*(x) \to T^*(x).$$

Linear dynamics on Hilbert spaces (Grivaux, Matheron, Menet 2017)

Studying typical properties of operators with respect to these topologies, they proved the existence of operators with particular dynamical properties.

Hypercyclicity

An operator T is said to be *hypercyclic* if there exists $x \in \mathcal{H}$ such that $\{x, T(x), T^2(x), \ldots\}$ is dense in $\mathcal{H}$.

Graphs, Girth, Chromatic Number

- A graph (non-oriented) $G = (V(G), E(G))$ is constituted of its set of vertices $V(G)$ and its set of edges $E(G)$ which is a symmetric subset of $V(G) \times V(G)$,

Graphs, Girth, Chromatic Number

- A graph (non-oriented) $G = (V(G), E(G))$ is constituted of its set of vertices $V(G)$ and its set of edges $E(G)$ which is a symmetric subset of $V(G) \times V(G)$,
- two vertices $v_1, v_2 \in V$ are said to be adjacent (written $v_1 \sim v_2$) if either (v_1, v_2) belongs to E,

Graphs, Girth, Chromatic Number

- A graph (non-oriented) $G = (V(G), E(G))$ is constituted of its set of vertices $V(G)$ and its set of edges $E(G)$ which is a symmetric subset of $V(G) \times V(G)$,
- two vertices $v_1, v_2 \in V$ are said to be adjacent (written $v_1 \sim v_2$) if either (v_1, v_2) belongs to E,

Definitions

- the girth of $g(G)$, G is the length of the shortest cycle in G,

Graphs, Girth, Chromatic Number

- A graph (non-oriented) $G = (V(G), E(G))$ is constituted of its set of vertices $V(G)$ and its set of edges $E(G)$ which is a symmetric subset of $V(G) \times V(G)$,
- two vertices $v_1, v_2 \in V$ are said to be adjacent (written $v_1 \sim v_2$) if either (v_1, v_2) belongs to E,

Definitions

- the girth of $g(G)$, G is the length of the shortest cycle in G,
- the chromatic number $\chi(G)$ of G is the minimal number of colors required to paint the vertices of G such that two adjacent vertices never have the same color,

Graphs, Girth, Chromatic Number

- A graph (non-oriented) $G = (V(G), E(G))$ is constituted of its set of vertices $V(G)$ and its set of edges $E(G)$ which is a symmetric subset of $V(G) \times V(G)$,
- two vertices $v_1, v_2 \in V$ are said to be adjacent (written $v_1 \sim v_2$) if either (v_1, v_2) belongs to E,

Definitions

- the girth of $g(G)$, G is the length of the shortest cycle in G,
- the chromatic number $\chi(G)$ of G is the minimal number of colors required to paint the vertices of G such that two adjacent vertices never have the same color,
- an independant set is a subset of $V(G)$ containing no two adjacent vertices. The *independance number* $\alpha(G)$ of G is the cardinal of its biggest independant set.

Graphs, Girth, Chromatic Number

- A graph (non-oriented) $G = (V(G), E(G))$ is constituted of its set of vertices $V(G)$ and its set of edges $E(G)$ which is a symmetric subset of $V(G) \times V(G)$,
- two vertices $v_1, v_2 \in V$ are said to be adjacent (written $v_1 \sim v_2$) if either (v_1, v_2) belongs to E,

Definitions

- the girth of $g(G)$, G is the length of the shortest cycle in G,
- the chromatic number $\chi(G)$ of G is the minimal number of colors required to paint the vertices of G such that two adjacent vertices never have the same color,
- an independant set is a subset of $V(G)$ containing no two adjacent vertices. The *independance number* $\alpha(G)$ of G is the cardinal of its biggest independant set.

A useful inequality: $\chi(G) \geq \dfrac{|V(G)|}{\alpha(G)}$.

Erdős's construction

High girth, high chromatic number

For any integers a and b, does there exist a finite graph G with $g(G) \geq a$ and $\chi(G) \geq b$?

Erdős's construction

High girth, high chromatic number

For any integers a and b, does there exist a finite graph G with $g(G) \geq a$ and $\chi(G) \geq b$?

- Consider the random graph $G_{n,p}$ with n vertices and where each potential edge appears independently with probability p.

Erdős's construction

High girth, high chromatic number

For any integers a and b, does there exist a finite graph G with $g(G) \geq a$ and $\chi(G) \geq b$?

- Consider the random graph $G_{n,p}$ with n vertices and where each potential edge appears independently with probability p.
- **Fact:** with p well-chosen, $G_{n,p}$ has a non-zero probability to have a "low" number of short cycles and a low independence number.

Erdős's construction

High girth, high chromatic number

For any integers a and b, does there exist a finite graph G with $g(G) \geq a$ and $\chi(G) \geq b$?

- Consider the random graph $G_{n,p}$ with n vertices and where each potential edge appears independently with probability p.
- **Fact:** with p well-chosen, $G_{n,p}$ has a non-zero probability to have a "low" number of short cycles and a low independence number.
- By removing a vertice from each short cycle of $G_{n,p}$, we end up with no short cycles and keep a low independence number.

Adjacency Matrix

Definition

The adjacency matrix M_G of a graph G is a square matrix in which the rows and columns are indexed by the vertices of G and defined by:

$$M_G(v, w) = \begin{cases} 1 & \text{if } v \sim w \\ 0 & \text{otherwise.} \end{cases}$$

- since we consider undirected graphs, M_G is always symmetric,
- $M_G^n(v, w)$ is equal to the number of paths of length n joining v and w.
- if M_G is d-regular then the biggest eigenvalue of M_G is d.

Spectral expansion

Assume that G is a connected d-regular graph.

A spectral measure of connectedness

If $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of M_G, define

$$\lambda(G) := \max_{|\lambda_i| \neq d} |\lambda_i| .$$

An element of explanation: $\lambda(G)$ measures how fast the Markov operator on the graph converges.

Ramanujan Graphs

Alon-Boppana theorem

When the number of vertices of G goes to infinity:

$$\lambda(G) \geq 2\sqrt{d-1} - o(1)$$

Ramanujan Graphs

Alon-Boppana theorem

When the number of vertices of G goes to infinity:

$$\lambda(G) \geq 2\sqrt{d-1} - o(1)$$

Ramanujan graphs

Ramanujan graphs are graphs for which $\lambda(G) \leq 2\sqrt{d-1}$.

- Complete graphs are Ramanujan. The interesting problem is to construct d-regular Ramanujan graphs of arbitrary size.
- *Expander* graphs are graphs for which λ does not go to d when the size of the graph goes to ∞.

A random answer

Random construction (Friedman 2003)

A random d-regular graph G is almost Ramanujan in the sense that when its size goes to ∞, with probability $1 - o(1)$,

$$\lambda(G) \leq 2\sqrt{d-1} + o(1).$$

The explicit construction

Let Γ be a group and S a symmetric generating set of Γ.

Cayley graph

The Cayley graph $G(\Gamma, S)$ is defined by

$$V(\Gamma, S) = \Gamma \text{ and } E(\Gamma, S) = \{(g, gs) : g \in \Gamma, s \in S\}.$$

The explicit construction

Let Γ be a group and S a symmetric generating set of Γ.

Cayley graph

The Cayley graph $G(\Gamma, S)$ is defined by

$$V(\Gamma, S) = \Gamma \text{ and } E(\Gamma, S) = \{(g, gs) : g \in \Gamma, s \in S\}.$$

Let p and q be two prime numbers with q large enough with respect to p and such that q is a square modulo p.

Margulis (1988), Lubotzky, Phillips, Sarnak (1988)

$X^{p,q} := G(PSL_2(\mathbb{F}_q), S_{p,q})$ is a $(p+1)$-regular Ramanujan graph.

Furthermore, $X^{p,q}$ has $\dfrac{q(q^2-1)}{2}$ vertices and

$$g(X^{p,q}) \geq 2 \log_p q.$$

Scheme of Proof

eigenvalues of M_G (G Ramanujan)

Scheme of Proof

eigenvalues of M_G (G Ramanujan)

$$\updownarrow$$

moments $m_k = tr(M_G^k)$

Scheme of Proof

$$\text{eigenvalues of } M_G \ (G \text{ Ramanujan})$$
$$\updownarrow$$
$$\text{moments } m_k = tr(M_G^k)$$
$$\updownarrow$$
$$\text{number of paths in } G$$

Scheme of Proof

$$\text{eigenvalues of } M_G \ (G \text{ Ramanujan})$$
$$\updownarrow$$
$$\text{moments } m_k = tr(M_G^k)$$
$$\updownarrow$$
$$\text{number of paths in } G$$
$$\updownarrow$$
$$\text{number of solution of a diophantine equation}$$

Scheme of Proof

eigenvalues of M_G (G Ramanujan)

$\updownarrow$

moments $m_k = tr(M_G^k)$

$\updownarrow$

number of paths in G

$\updownarrow$

number of solution of a diophantine equation

$\updownarrow$

coefficients in the q-expansion of a certain modular form

Scheme of Proof

eigenvalues of M_G (G Ramanujan)

$\updownarrow$

moments $m_k = tr(M_G^k)$

$\updownarrow$

number of paths in G

$\updownarrow$

number of solution of a diophantine equation

$\updownarrow$

coefficients in the q-expansion of a certain modular form

Where the name comes from

The growth of these coefficients is controled by a conjecture of Ramanujan, the last ingredient of which was proved by Deligne (1974).

To conclude on this example

An interpretation:

- Some typical behaviours are difficult to reproduce with deterministic formulas (in this case: determination $\to$ order $\to$ bad connectedness)

To conclude on this example

An interpretation:

- Some typical behaviours are difficult to reproduce with deterministic formulas (in this case: determination $\rightarrow$ order $\rightarrow$ bad connectedness)
- Number theory provides the required level of "randomness" (erratic behaviour of prime numbers) and control (deep estimates obtained through monumental collective work) to reproduce these typical behaviours.

Noncommutative probability

In classical probability, the distribution of a random variable is determined by its moments (Levy's theorem).

Noncommutative probability

In classical probability, the distribution of a random variable is determined by its moments (Levy's theorem).

Joint distribution of matrices

The joint distribution of matrices $M_1, \ldots, M_d$ is defined as the collection of their joint moments:

$$m_{i_1,\ldots,i_m} = \frac{1}{n} tr(M_{i_1} \ldots M_{i_m}) \text{ for any } m \in \mathbb{N} \text{ and } i_1, \ldots, i_m \in \{1, \ldots, d\}^m.$$

Freeness

In this context, the usual notion of *independance* is replaced by *freeness*.

Large random matrices

Freeness describes the behaviour of many models of large random matrices, meaning that as the size of the matrices goes to infinity, their moments converge to those of free operators.

Random Unitaries and Freeness

Let $U_1, \ldots, U_d$ be random independent unitary (or permutation, or matching) matrices in dimension n.

Haagerup, Thorbjornsen (2005), Bordenave, Collins (2019)

The matrices $U_1, \ldots, U_d$ strongly converge to free unitaries as n goes to ∞.

Random Unitaries and Freeness

Let $U_1, \ldots, U_d$ be random independent unitary (or permutation, or matching) matrices in dimension n.

Haagerup, Thorbjornsen (2005), Bordenave, Collins (2019)

The matrices $U_1, \ldots, U_d$ strongly converge to free unitaries as n goes to ∞.

Consequences

- For any noncommutative polynomial P the behaviour of

$$\|P(U_1, \ldots, U_d)\|$$

  can be predicted assymptotically.

Random Unitaries and Freeness

Let $U_1, \ldots, U_d$ be random independent unitary (or permutation, or matching) matrices in dimension n.

Haagerup, Thorbjornsen (2005), Bordenave, Collins (2019)

The matrices $U_1, \ldots, U_d$ strongly converge to free unitaries as n goes to ∞.

Consequences

- For any noncommutative polynomial P the behaviour of
$$\|P(U_1, \ldots, U_d)\|$$
can be predicted assymptotically.
- In particular (connection to Ramanujan graphs),
$$\left\|\sum_{i\leq k} U_i\right\| \to 2\sqrt{d-1} \text{ almost surely.}$$

Open questions

A deterministic model

Can we construct an explicit sequence of matrices which is asymptotically strongly free?

Open questions

A deterministic model

Can we construct an explicit sequence of matrices which is asymptotically strongly free? Could it be done through number theoretic arguments?

Open questions

A deterministic model

Can we construct an explicit sequence of matrices which is asymptotically strongly free? Could it be done through number theoretic arguments?

Back to Ramanujan graphs

It is still not known whether 7-regular non-bipartite Ramanujan graphs of arbitrary size exist.

The bipartite case is entirely solved (though not by a completely explicit construction) by Marcus, Spielman and Srivastava (2015).

J'aime ma Vouvou !!!