The dichotomy between structure and randomness

International Congress of Mathematicians, Aug 23 2006

Terence Tao (UCLA)

2. Structure theorem: Every object is a superposition of a structured object and a pseudorandom error.

- Spectral decomposition: Objects decompose into almost periodic (discrete spectrum) and mixing (continuous spectrum) components.
- Littlewood-Paley decomposition: Objects decompose into low-frequency (coarse-scale) and high-frequency (fine-scale) components.
- Szemerédi regularity lemma: Graphs decompose into low-complexity partitions and regular graphs between partition classes.

Structure theorems are often established via a stopping time argument based on iterating a **dichotomy**. They combine well with the **negligibility** of the pseudorandom error.

3. **Rigidity:** If an object is approximately structured, then it is close to an object which is perfectly structured.

- Additive inverse theorems: If a set A is approximately closed under addition, then it is close to a group, convex body, an arithmetic progression, or a combination thereof. (Freiman, ...)
- Compactness of minimising sequences: Approximate minimisers of a functional tend to be close to exact minimisers. (Palais-Smale, ...)
- Property testing: If random samples of a graph or function satisfy certain types of properties locally, then it is likely to be close to a graph or function which satisfies the property globally.

Rigidity theorems are often quite deep; for instance **structure theorems** are often used in the proof.

4. **Classification:** Perfectly structured objects can be described explicitly and algebraically/geometrically.

- Simple examples: the classification of finitely generated abelian groups, linear transformations, or quadratic forms via suitable choices of basis.
- A more advanced example: the algebro-geometric description of soliton or multisoliton solutions to completely integrable equations (such as the Korteweg-de Vries equation).
- A recent example: description of the minimal characteristic factor for multiple recurrence via nilsystems. (Host-Kra 2002, Ziegler 2004)

Classification results tend to rely more on algebra and geometry than on analysis, and can be very difficult to establish.

Model example: Szemerédi's theorem

Every subset A of the integers of positive (upper) density $\overline{\delta}[A] > 0$ contains arbitrarily long arithmetic progressions.

- Many deep and important proofs: Szemerédi (1975), Furstenberg (1977), Gowers (1998), ...
- Main difficulty: A could be very structured, very pseudorandom, or a hybrid of both. The set A always has long arithmetic progressions, but for different reasons in each case.

What does structure mean here? Some examples:

- Periodic sets: $A = \{100n : n \in \mathbb{Z}\}$;
- Quasiperiodic sets: $A = \{n : \mathrm{dist}(\sqrt{2}n, \mathbb{Z}) \leq \frac{1}{200}\}$;
- Quadratically quasiperiodic sets: $A = \{n : \mathrm{dist}(\sqrt{2}n^2, \mathbb{Z}) \leq \frac{1}{200}\}$.

The precise definition of structure depends on the length of the progression one is seeking.

Key observation: If many terms in an arithmetic progression lie in a structured set A, then the next term in the progression is very likely to lie in A (i.e. strong positive correlation).

Thus progressions are created in this case by algebraic structures, such as periodicity.

What does pseudorandomness mean here? Some examples:

- Random sets: $\mathbb{P}(n \in A) = \frac{1}{100}$ for each n, independently at random.
- Discorrelated sets: Sets with small correlations, e.g. $\overline{\delta}(A \cap (A+k)) \approx \overline{\delta}(A)\overline{\delta}(A+k)$ for most k.

The precise definition of pseudorandomness depends on the length of the progression one is seeking.

Probability theory lets one place long progressions in A with positive probability provided one has sufficiently strong control on correlations (Gowers uniformity). Thus progressions are created in this case by discorrelation.

What does hybrid mean here? Some examples:

- Pseudorandom subsets of structured sets: $\frac{1}{50}$ of the even numbers, chosen independently at random.
- Pseudorandom subsets of structured partitions: $\mathbb{P}(n \in A) = p_1$ when n is even and $\mathbb{P}(n \in A) = p_2$ when n is odd, for some probabilities $0 \leq p_1, p_2 \leq 1$.

Since structured sets are already known to have progressions, a pseudorandom subset of such sets will have a proportional number of such progressions. Thus progressions are created in this case by a combination of algebraic structure and discorrelation.

How to generalise the above arguments to arbitrary sets? This requires

Structure theorem: An arbitrary dense set A will always contain a large component which is a pseudo-random subset of a structured set.

This in turn follows from

Dichotomy: If a set does not behave pseudorandomly, then it correlates with a nontrivial structured object (e.g. it has increased density on a long subprogression).

A variant: the Green-Tao theorem (2004)

The primes contain arbitrarily long progressions.

- The primes are conjectured to behave pseudorandomly after accounting for local obstructions (Hardy-Littlewood prime tuples conjecture). This conjecture would imply the above theorem (as well as many other conjectures concerning the primes).

- It is known that the primes behave Fourier-pseudorandomly after accounting for local obstructions (Vinogradov's method). This already gives infinitely many progressions of primes of length 3 (Hardy-Littlewood circle method). Unfortunately, it does not say much about higher length progressions.

- The primes are too sparse for Szemerédi's theorem to apply directly.
- However, the primes are a dense subset of the almost primes (numbers with few prime factors), which were known to be very pseudorandomly distributed after accounting for local obstructions (sieve theory). We can exploit this by using

> **Relative Szemerédi theorem:** Every subset of a pseudorandom set of integers of positive relative density contains arbitrarily long arithmetic progressions.

- This lets us finesse the question of whether the primes are pseudorandom or not; they merely need to be a dense subset of a pseudorandom set.

A basic problem that occurs in many areas of analysis, combinatorics, PDE, and applied mathematics is the following:

> The space of all objects in a given class is usually very high (or infinite) dimensional.

Examples: subsets of N points; graphs on N vertices; functions on N values; systems with N degrees of freedom.

- The "curse of dimensionality" (large data is expensive to analyse)
- Failure of compactness (local control does not imply global control; lack of convergent subsequences)
- Inequivalence of norms (control in norm X does not imply control in norm Y)
- Unbounded complexity (objects have no usable structure)

To prove the **relative Szemerédi theorem**, we need to combine the ordinary **Szemerédi theorem** with two facts:

Structure theorem: Dense subsets of sparse pseudorandom sets contain a large component which is a sparse pseudorandom subset of a dense set.

Negligibility: Sparse pseudorandom subsets of a set will contain a proportional number of arithmetic progressions.

The **Structure theorem** in turn follows from iterating

Dichotomy: If a dense subsets of pseudorandom sets is not pseudorandom, it correlates with a dense structured set.

More precise asymptotics

- **Szemerédi's theorem** and the **Green-Tao theorem** show that certain sets contain many progressions of any given length. But they do not quantify exactly how many progressions there are, for instance:

> **Question**: How many progressions of length k are there among the prime numbers less than N, as $N \to \infty$?

- The precise number of progressions depends on the exact decomposition of the set into structured and pseudorandom components. No matter what the decomposition, one always has some progressions, but different decompositions can lead to different numbers of progressions.

- To answer the above **question** (and when counting more general types of additive patterns within the primes), it is not enough to know abstractly that the primes decompose into structured and pseudorandom components; one needs to know precisely what these components are.
- To do this one needs to use some deeper facts about structure and pseudorandomness, such as the **classification** of perfectly structured objects.

van der Corput's theorem (1927): The number of progressions of length 3 in the primes less than N is

$$\left[\frac{1}{2}\prod_{p\geq 3}(1-\frac{2}{p})(\frac{p}{p-1})^2 + o(1)\right]\frac{N^2}{\log^3 N}.$$

- To prove this, it suffices by the Hardy-Littlewood circle method to show that the primes are Fourier-pseudorandom after accounting for local obstructions (major arcs); this allows us to **neglect** the contribution of the minor arcs.
- In the Fourier-analytic case, the structured objects are completely **classified**: they are characters.
- By the **dichotomy**, we thus need to show that the primes do not correlate with minor arc characters. This can be done by Vinogradov's method.

More recently, asymptotics have become available for other additive patterns in the primes, such as arithmetic progressions of length 4.

- For these more complex patterns, Fourier-pseudorandomness is not enough; one needs to establish Gowers uniformity of the primes (after accounting for local obstructions) in order to **neglect** all non-local effects.
- The corresponding structured objects have been recently **classified** as nilsequences arising from flows on a quotient of a nilpotent Lie group.
- By the **dichotomy**, we thus need to show that the primes do not correlate with "minor arc" nilsequences. This can be done by a refined version of Vinogradov's method.

(For details, see the lecture of Ben Green.) ◇

But in many cases, this basic problem can be resolved by the following phenomenon:

> One can often reduce the analysis to the space of effective objects in a given class, which is typically low-dimensional, compact, or classifiable.

Examples:

- Parabolic theory (Compact attractors, Littlewood-Paley, Hamilton/Perelman, …)
- Concentration-compactness (Lions, …)
- Graph structure theorems (Szemerédi, …)
- Ergodic structure theorems (von Neumann, Furstenberg, …)
- Additive structure theorems (Freiman, Balog-Szemerédi-Gowers, Gowers, …)
- Signal processing (compression, denoising, homogenisation, …)

Structure vs. randomness

To understand this phenomenon one must consider two opposing types of mathematical objects, which are analysed by very different tools:

- Structured objects (e.g. periodic or low-frequency functions or sets; low-complexity graphs; compact dynamical systems; solitary waves); and
- Pseudorandom objects (e.g. random or high-frequency functions, sets, or graphs; mixing dynamical systems; radiating waves).

Defining these classes precisely is an important and nontrivial challenge, and depends heavily on the context.

Structured	Pseudorandom
Compact	Generic
Periodic (self-correlated)	Mixing (discorrelated)
Low complexity/entropy	High complexity/entropy
Coarse-scaled (smooth)	Fine-scaled (rough)
Predictable (signal)	Unpredictable (noise)
Measurable ($\mathbb{E}(f\|\mathcal{B}) = f$)	Martingale ($\mathbb{E}(f\|\mathcal{B}) = 0$)
Concentrated (solitons)	Dispersed (radiation)
Discrete spectrum	Continuous spectrum
Major arc (rational)	Minor arc (Diophantine)
Eigenfunctions (elliptic)	Spectral gap (dynamic)
Algebra (=)	Analysis (<)
Geometry	Probability

0. **Negligibility:** For the purposes of statistics (e.g. averages, integrals, sums), the pseudorandom components of an object are asymptotically negligible.

- Generalised von Neumann theorems: Functions which are sufficiently mixing have no impact on asymptotic multiple averages. (Furstenberg, ...)
- Perturbation theory: Perturbations which are sufficiently dispersed have negligible impact on nonlinear PDE.
- Counting lemmas: Graphs which are sufficiently regular have statistics which are a proportional fraction of the statistics of the complete graph.

These **negligibility** results are typically proven using harmonic analysis methods, ranging from the humble Cauchy-Schwarz inequality to more advanced estimates.

Because of this **negligibility**, we would like to be able to easily locate the structured and pseudorandom components of a given object.

> **Typical conjecture:** "Natural" objects behave pseudorandomly after accounting for all the obvious structures.

These conjectures can be extremely hard to prove!

- The primes should behave randomly after accounting for "local" (mod p) obstructions. (Hardy-Littlewood prime tuples conjecture; Riemann hypothesis; …)
- Solutions to highly nonlinear systems should behave randomly after accounting for conservation laws etc. (Rigorous statistical mechanics; ?Navier-Stokes global regularity?; …)
- There should exist "describable" algorithms which behave "unpredictably". ($P = BPP$; ?$P \neq NP$?; …)

- With current technology, we often cannot distinguish structure from pseudorandomness directly.
- However, we are often fortunate to possess four weaker, but still very useful, principles concerning structure and pseudorandomness...

1. **Dichotomy:** An object is not pseudorandom if and only if correlates with a structured object (or vice versa).

- Lack of uniform distribution can often be traced to a large Fourier coefficient. (Weyl, Erdős-Turán, Hardy-Littlewood, Roth, Gowers, ...)
- Lack of mixing can often be traced to an eigenfunction. (Koopman-von Neumann, ...)
- Lack of dispersion can often be traced to a bound state or large wavelet coefficient.

Such **dichotomies** are often established via some kind of spectral theory or Fourier analysis (or generalisation thereof).