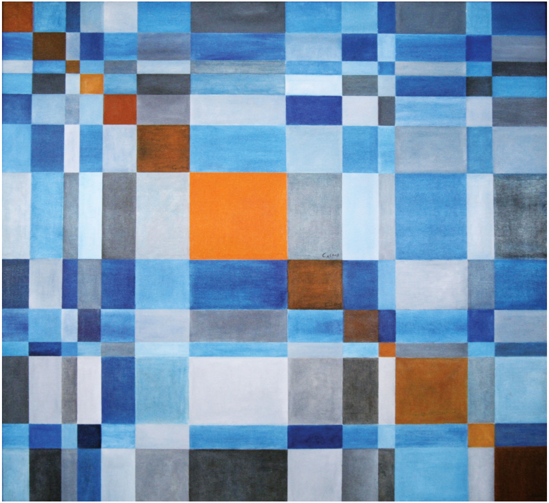
Diagonalize This

Iian Smythe

Department of Mathematics
Cornell University

Olivetti Club
November 26, 2013



"Surprised Again on the Diagonal", Lun-Yi Tsai, 2002,
Permanent Collection, Butler Institute of American Art

Cantor's Theorem

In his 1874 paper, Georg Cantor gave birth to set theory with the following result:

Theorem (Cantor)

The set of real numbers is uncountable.

In order to prove this result, Cantor showed that given any countable list of real numbers $\{r_n : n \in \mathbb{N}\}$, there is a real number r which does not occur in this list, i.e., for all $n \in \mathbb{N}$, $r \neq r_n$.

How do we *build* such an r?

Cantor's Theorem: Take I

One way to build a real number is to define a decreasing, nested sequence of nonempty closed intervals $\{[a_n, b_n]\}_{n=0}^{\infty}$ whose lengths go to zero. The real number this corresponds to is the unique r such that $\{r\} = \bigcap_{n=0}^{\infty}[a_n, b_n]$.

Denote by $\mathcal{I} = \{[a, b] \subseteq \mathbb{R} : b - a > 0\}$, the set of nontrivial closed intervals in $\mathbb{R}$.

Observe that if $[a, b] \in \mathcal{I}$, then for any real number r_0, and $n > 0$, there is an $[a_0, b_0] \in \mathcal{I}$ with $b_0 - a_0 < \frac{1}{n}$ and $r_0 \notin [a_0, b_0]$.

Cantor's Theorem: Take I (cont'd)

Proof. (Cantor, 1874).

Let $\{r_n\}_{n\in\mathbb{N}}$ be a countable list of real numbers. We will produce an r not on this list, thus showing that $\mathbb{R}$ is uncountable.

Define sets $[a_n, b_n] \in \mathcal{I}$ by recursion:
Let $[a_0, b_0]$ be any interval in $\mathcal{I}$ with $r_0 \notin [a_0, b_0]$.
Given $[a_k, b_k]$, let $[a_{k+1}, b_{k+1}]$ be any interval in $\mathcal{I}$ such that $[a_{k+1}, b_{k+1}] \subseteq [a_k, b_k]$, $r_{k+1} \notin [a_{k+1}, b_{k+1}]$, and $b_{k+1} - a_{k+1} < \frac{1}{k+1}$.

By construction, $\{[a_n, b_n]\}_{n=0}^{\infty}$ is a nested sequence of nonempty closed intervals whose length goes to zero, and for every n, $r_n \notin [a_n, b_n]$. Taking r to be the unique real number such that $\{r\} = \bigcap_{n=0}^{\infty}[a_n, b_n]$, then $r \neq r_n$ for any n, as desired. □

Cantor's Theorem: Take II

By identifying real numbers with infinite binary sequences, another way to build a real number is to define a sequence of finite binary strings $\{\sigma_n\}_{n=0}^{\infty}$ such that $\sigma_{n+1} \supseteq \sigma_n$, i.e., σ_{n+1} *extends* σ_n for each n, and the length of the σ_n, denoted by $|\sigma_n|$, goes to ∞. The real number (i.e., infinite binary sequence) this corresponds to is $x = \bigcup_{n=0}^{\infty} \sigma_n$.

Let $2^{<\omega}$ be the set of all finite binary sequences, which we may think of as functions from finite initial segments of $\mathbb{N}$ to $\{0, 1\}$. Infinite binary sequences are (total) functions from $\mathbb{N}$ to $\{0, 1\}$.

Observe that if $\sigma \in 2^{<\omega}$, then for any infinite binary sequence x_0 and $n > 0$, there is a $\sigma_0 \in 2^{<\omega}$ which extends σ with $|\sigma_0| > n$, and for some $m \in \mathrm{dom}(\sigma_0)$, $\sigma_0(m) \neq x_0(m)$.

Cantor's Theorem: Take II

Proof. (essentially Cantor, 1891).

Let $\{x_n : n \in \mathbb{N}\}$ be a countable list of infinite binary sequences. We will produce an x not on this list, thus showing that $\mathbb{R}$ is uncountable.

Define binary strings $\sigma_n \in 2^{<\omega}$ by recursion:
Let σ_0 be any sufficiently long binary string such that for some $m \in \mathrm{dom}(\sigma_0)$ for which $\sigma_0(m) \neq x_0(m)$.
Given σ_k, let σ_{k+1} extend σ_k such that $|\sigma_{k+1}| > k + 1$, and there is some $m \in \mathrm{dom}(\sigma_{k+1})$ for which $\sigma_{k+1}(m) \neq x_{k+1}(m)$.

By construction, $\{\sigma_n\}_{n=0}^{\infty}$ is sequence of binary strings, each extending the next, and such that for each n, $|\sigma_n| > n$ and there is some $m \in \mathrm{dom}(\sigma_n)$ such that $\sigma_n(m) \neq x_n(m)$. Taking $x = \bigcup_{n=0}^{\infty} \sigma_n$, we have that $x \neq x_n$ for any n, as desired. □

A generic framework

Each of these constructions consists of a partially ordered set:

$\mathcal{I} = \{[a,b] \subseteq \mathbb{R} : b - a > 0\}$ ordered by $[a,b] \leq [a',b']$ iff $[a,b] \subseteq [a',b']$

$2^{<\omega}$ ordered by $\sigma' \leq \sigma$ iff $\sigma' \supseteq \sigma$ (*reverse* inclusion)

Given these, we constructed a decreasing sequence of elements which approximates the desired object (a real number). By using a limiting operation (intersection, union), we obtain the desired object.

A generic framework (cont'd)

Definition

Let $\mathbb{P}$ be a partially ordered set. A subset $D \subseteq \mathbb{P}$ is *dense* if for every $p \in \mathbb{P}$, there is a $q \in D$ with $q \leq p$.

In $\mathcal{I}$, for each n and each fixed real number r_0, the set

$$D_{n,r_0} = \{[a,b] \in \mathcal{I} : r_0 \notin [a,b] \text{ and } b - a < \frac{1}{n}\}$$

is dense.

In $2^{<\omega}$, for each n and each fixed infinite binary sequence x_0, the set

$$D_{n,x_0} = \{\sigma \in 2^{<\omega} : \exists m(m \in \operatorname{dom}(\sigma) \text{ and } \sigma(m) \neq x_0(m)) \text{ and } |\sigma| > n\}$$

is dense.

A generic framework (cont'd)

We can think of a dense set $D \subseteq \mathbb{P}$ as specifying properties which are true "generically", i.e., *most* objects being approximated by elements of $\mathbb{P}$ should satisfy those properties.

The examples we've seen correspond to the fact that given any fixed real number, most real numbers differ from it. So, differing from that real number is a *generic* property, as is differing from any given countable list of real numbers.

This motivates the following definition:

Definition

Let $\mathcal{D}$ be a collection of dense subsets of a partially ordered set $\mathbb{P}$. A decreasing sequence $\{p_n\}_{n=0}^{\infty}$ of elements of $\mathbb{P}$ such that for each $D \in \mathcal{D}$, there exists an n for which $p_n \in D$, is said to be $\mathcal{D}$-*generic*.

A key lemma

The following lemma generalizes our constructions.

Lemma (Rasiowa-Sikorski)

Let $\mathbb{P}$ be a partially ordered set, and $\mathcal{D}$ a countable collection of dense subsets of $\mathbb{P}$. For any $p \in \mathbb{P}$, there exists a decreasing, $\mathcal{D}$-generic sequence $\{p_n\}_{n=0}^{\infty}$ such that $p_0 = p$.

Proof.

Let $\mathcal{D} = \{D_n : n \in \mathbb{N}\}$ and $p \in \mathbb{P}$ be given. Define p_n by recursion:
Put $p_0 = p$. Given p_k, let $p_{k+1} \leq p_k$ with $p_{k+1} \in D_k$. We can always find such a p_{k+1} because D_k is dense.
By construction, $\{p_n\}_{n=0}^{\infty}$ is decreasing and $\mathcal{D}$-generic. □

Baire's Theorem

Theorem (Baire)

If $\{G_n\}_{n=0}^{\infty}$ is a sequence of dense open subsets of $\mathbb{R}$, then $G = \bigcap_{n=0}^{\infty} G_n$ is dense in $\mathbb{R}$.

Proof.

Fix $V \subseteq \mathbb{R}$ open and nonempty. It suffices to show that $G \cap V \neq \emptyset$. By shrinking V, we may assume that $\overline{V}$ is compact.
Let $\mathbb{P} = \{U \subseteq V : U$ open, nonempty, $\overline{U} \subseteq V\}$, ordered by containment.
For each n, let $D_n = \{U \in \mathbb{P} : \overline{U} \subseteq G_n\}$, and $\mathcal{D} = \{D_n : n \in \mathbb{N}\}$.
Since each G_n is dense open, if $U \in \mathbb{P}$, there is a small open interval I such that $\bar{I} \subseteq U \cap G_n$, so $I \in D_n$ and $I \leq U$, witnessing that D_n is dense.
Applying the lemma, let $\{U_n\}_{n=0}^{\infty}$ be a $\mathcal{D}$-generic sequence. Since $\overline{V}$ is compact, $\bigcap_{n=0}^{\infty} \overline{U_n}$ is nonempty. Taking $x \in \bigcap_{n=0}^{\infty} \overline{U_n}$, we see that $x \in G \cap V$ as desired. □

Continuous nowhere-differentiable functions

Theorem (Weierstrass, Banach)

There exists functions in $C([0,1])$ which are nowhere-differentiable.

Proof.

Let $\mathbb{P} = \{U \subseteq C([0,1]) : U$ is open and nonempty$\}$. For each n, m, let $D_{n,m}$ be the set of all $U \in \mathbb{P}$ such that for all $f \in U$,

$$\forall x \in [0,1] \exists t \in [0,1] \left(0 < |x - t| < 1/m \text{ and } \left| \frac{f(x) - f(t)}{x - t} \right| > n \right).$$

One can show that the sets $D_{n,m}$ are dense in $\mathbb{P}$. Combining these with sets $D^k = \{U \in \mathbb{P} : \operatorname{diam}(U) < \frac{1}{k}\}$, we get a countable collection of dense sets $\mathcal{D}$. If $\{U_n\}_{n=0}^{\infty}$ is a $\mathcal{D}$-generic sequence, and f is the unique element of $C([0,1])$ such that $\{f\} = \bigcap_{n=0}^{\infty} \overline{U_n}$, then f is a continuous function which is nowhere differentiable. □

Countable dense linear orders

Theorem (Cantor)

Every two countable dense linear orders without endpoints are isomorphic, and in particular, are isomorphic to $\mathbb{Q}$.

Proof.

Fix such a linear order L. Let $\mathbb{P}$ be the set of all partial embeddings of L into $\mathbb{Q}$, ordered by reverse inclusion.

Consider sets $B_a = \{p \in \mathbb{P} : a \in \mathrm{dom}(p)\}$ where $a \in L$, and $F_r = \{p \in \mathbb{P} : r \in \mathrm{ran}(p)\}$ where $r \in \mathbb{Q}$. It is easy to check that these sets are dense in $\mathbb{P}$. Let $\mathcal{D}$ consists of all the B_a and F_r.

Since L and $\mathbb{Q}$ are countable, there is a $\mathcal{D}$-generic sequence $\{p_n\}_{n=0}^{\infty}$ in $\mathbb{P}$. Then, $f = \bigcup_{n=0}^{\infty} p_n$ must be an isomorphism of L onto $\mathbb{Q}$. □

Where do we go from here?

The technique of building generic sequences for countable collections of dense sets can be used in a variety of mathematical disciplines.

- Sets of natural numbers with incomparable “information content”, the nonuniformity of the P vs NP question (see: recursion theory, complexity theory)
- Further consequences of Baire’s theorem such as functions with divergent Fourier series, automatic continuity of certain classes of homomorphisms (see: functional analysis, descriptive set theory)
- Isomorphisms between certain countable ordered or algebraic structures (see: order theory, model theory)

More dense sets?

A natural question is whether we can meet more (i.e., uncountably many) dense sets in these constructions. Sequences will not work for this purpose.

Definition

Given a partially ordered set $\mathbb{P}$, a subset $F \subseteq \mathbb{P}$ is a *filter* if it is nonempty and satisfies

- if $p \in F$ and $p \leq q$, then $q \in F$, and
- if $p, q \in F$, then there is a $r \in F$ such that $r \leq p, q$.

It is easy to check that the upwards closure of a chain is a filter.

One can also show that the union of a filter of partial functions (e.g., in $2^{<\omega}$) is still a (partial) function, and that the intersection of a filter of nonempty compact sets is nonempty, preserving two properties we have used for decreasing sequences in such partial orders.

More dense sets? (cont'd)

Definition

Let $\mathcal{D}$ be a collection of dense subsets of partially ordered set $\mathbb{P}$. A filter $G \subseteq \mathbb{P}$ is *$\mathcal{D}$-generic* if for every $D \in \mathcal{D}$, there is a $p \in G \cap D$.

Since the upwards closure of a $\mathcal{D}$-generic sequence is a $\mathcal{D}$-generic filter, it is clear that the Rasiowa-Sikorski Lemma allows us to build $\mathcal{D}$-generic filters for countable $\mathcal{D}$.

So, we can ask our question more precisely: Given an uncountable collection $\mathcal{D}$ of dense subsets of a partially ordered set $\mathbb{P}$, is there a $\mathcal{D}$-generic filter?

More dense sets? (cont'd)

In general, the answer is no:

Let $\mathbb{P} = 2^{<\omega}$. If $\mathcal{D} = \{D_x : x \in 2^\omega\}$, where for each infinite binary string x, $D_x = \{\sigma \in 2^{<\omega} : \exists m(m \in \mathrm{dom}(\sigma)$ and $\sigma(m) \neq x(m))\}$, then $\mathcal{D}$ is a (size $2^{\aleph_0}$) collection of dense subsets of $2^{<\omega}$ for which there can be no generic filter.

If there was such a filter $G \subseteq \mathbb{P}$, then $y = \bigcup_{\sigma \in G} \sigma$ would be an infinite binary string such that $y \neq x$ for all infinite binary strings x, a contradiction.

We flew too close to the sun, and tried to diagonalize against *every* real number, leading to absurdity.

Can we find a way around this?

Forcing

We can cheat.

A standard result in mathematical logic (the Löwenheim-Skolem-Tarski Theorem) states that every consistent first-order theory (i.e., set of axioms) has a *countable* model.

A variation on this will allow us to consider *countable* models of ZFC set-theory. That is, countable structures M which satisfy the axioms of ZFC, and thus are *toy universes* in which *all* of mathematics can be simulated.

In particular, such an M has its own (countable) copies of the natural numbers, the real numbers, functions on the real numbers, etc, the latter two of which M thinks are uncountable, i.e., there are no functions from the natural numbers onto them *within* M.

Forcing (cont'd)

Granting the existence of such countable models M, we can "diagonalize against all of the reals", at least those in M.

In M, consider $\mathbb{P} = 2^{<\omega}$, and $\mathcal{D} = \{D_x : x \in (2^\omega)^M\}$, where $D_x = \{\sigma \in 2^{<\omega} : \exists m(m \in \mathrm{dom}(\sigma)$ and $\sigma(m) \neq x(m))\}$.

Viewed externally, $\mathcal{D}$ is countable since M is. Thus, there exists a $\mathcal{D}$-generic filter G, and so $y = \bigcup_{\sigma \in G} \sigma$ is an infinite binary string which *cannot* be in M.

In other words, we've built a *new* real number, at least from the persecutive of M.

Notice that since M is countable, there are only countably many dense subsets of $\mathbb{P}$ in M of any kind, so we actually could have met all of them with a single filter G, called an *M-generic*.

Forcing and the Continuum Hypothesis

Cohen showed that given an M-generic filter G, there is a model $M[G]$, called a *generic extension* of M, such that $M \subseteq M[G]$ and $G \in M[G]$. This technique is called *forcing*, since $\mathbb{P}$ will "force" what is true in $M[G]$.

Forcing with (essentially) κ-many copies of $2^{<\omega}$, where κ is a cardinal number in M greater than the least uncountable one ($\aleph_1$), Cohen proved the consistency of the negation of the continuum hypothesis:

Theorem (Cohen)

If M is a countable transitive model of ZFC*, then there is a partially ordered set $\mathbb{P} \in M$ and an M-generic filter G such that in $M[G]$ the cardinality of real numbers is greater than $\aleph_1$.*

Forcing axioms

Since its inception in the early 1960's, forcing has become a fundamental technique in set theory.

However, understanding forcing requires dealing with many meta-mathematical/meta-logical unpleasantries surrounding the existence of countable transitive models.

An alternate way to use these techniques is to take, as additional axioms, the ability to meet certain uncountable collections of dense sets for "nice" partially ordered sets, provided you (or someone else) can prove these axioms consistent (by forcing).

These are the so-called *forcing axioms*.

Forcing axioms (cont'd)

The first and most utilized forcing axiom is due to Martin:

Definition

For $\aleph_0 \leq \kappa < 2^{\aleph_0}$, (MA_κ) is the statement:
"For any *ccc* partially ordered set $\mathbb{P}$, if $\mathcal{D}$ is a collection of dense subsets of $\mathbb{P}$ for which $|\mathcal{D}| \leq \kappa$, then there there is a $\mathcal{D}$-generic filter."

Here "ccc" (the *countable chain condition*) is a niceness condition for $\mathbb{P}$, and we restrict to $\kappa < 2^{\aleph_0}$ because, as we have already seen, we cannot meet $2^{\aleph_0}$ many dense sets within our universe.

Replacing "ccc" with other niceness conditions, e.g., "σ-centered", "proper", "preserving stationary subsets of ω_1"... yields different forcing axioms: $\text{MA}_{\sigma\text{-centered}}$, PFA, MM,...

Forcing axioms (cont'd)

Forcing axioms are often called "strong forms of Baire's theorem" for the following reason:

Theorem

(MA$_\kappa$) *If* $\{G_\alpha : \alpha < \kappa\}$ *is a collection of dense open subsets of* $\mathbb{R}$*, then* $G = \bigcap_{\alpha<\kappa} G_\alpha$ *is dense in* $\mathbb{R}$*.*

Proof.

Fix $V \subseteq \mathbb{R}$ open and nonempty. It suffices to show that $G \cap V \neq \emptyset$. By shrinking V, we may assume that $\overline{V}$ is compact.
Let $\mathbb{P} = \{U \subseteq V : U$ open, nonempty, $\overline{U} \subseteq V\}$, ordered by containment.
For each $\alpha < \kappa$, let $D_\alpha = \{U \in \mathbb{P} : \overline{U} \subseteq G_\alpha\}$, and $\mathcal{D} = \{D_\alpha : \alpha \in \mathbb{N}\}$.
Exactly as before, each D_α is dense in $\mathbb{P}$.
Applying MA$_\kappa$, let $\mathcal{G}$ be a $\mathcal{D}$-generic filter. Since $\overline{V}$ is compact, $\bigcap_{U\in\mathcal{G}} \overline{U}$ is nonempty. Taking $x \in \bigcap_{U\in\mathcal{G}} \overline{U}$, we see that $x \in G \cap V$ as desired. □

Forcing axioms (cont'd)

MA$_\kappa$ has many interesting consequences for the structure of $\mathbb{R}$:

- The intersection of κ-many dense open subsets of $\mathbb{R}$ is dense.
- The union of κ-many measure zero subsets of $\mathbb{R}$ is measure zero.
- (for $\kappa = \aleph_1$) (Solovay-Tennenbaum) $\mathbb{R}$ is the unique complete dense linear order without endpoints such that that every collection of disjoint, non-trivial intervals is countable.
- (Martin-Solovay) $\kappa < 2^{\aleph_0}$ but $2^\kappa = 2^{\aleph_0}$.

Thanks for listening!