The Cantor Set

A course at the Nesin Matematik Köyü

David Pierce

January 23–9, 2017
Last edited, February 6, 2017

Matematik Bölümü
Mimar Sinan Güzel Sanatlar Üniversitesi
İstanbul
mat.msgsu.edu.tr/~dpierce/
dpierce@msgsu.edu.tr

Preface

The present typeset document is based on my course "The Cantor Set," January 23–9 (Monday–Sunday), 2017, 11:00–13:00. The fundamental idea is the existence of a bijection from the power set of the natural numbers, with the Tychonoff topology, to the Cantor Ternary Set, with the Euclidean topology inherited from the real numbers. Named theorems proved include the following.

Cantor's Theorem. The power set of a set is strictly larger than the set itself (Theorem 5, page 8).

The Heine–Borel Theorem (for $\mathbb{R}$ only; Theorem 7, page 17).

The Compactness Theorem (for propositional logic; Theorem 10, page 21: effectively, the simplest nontrivial case of the Tychonoff Theorem for infinite products).

The Stone Representation Theorem. Every Boolean algebra embeds in a power set (Theorem 17, page 33).

I spoke mostly in Turkish, while writing in English. Twenty-five students registered, but attendence dropped below ten by the fourth day. On the last day, there were four students, and I was sick with the flu virus that had been going around; I spoke for only an hour.

I started typesetting this document after the first lecture. Sources include (1) my handwritten notes, prepared before the lectures, (2) my memory of what happened in the lectures, (3) my typeset notes for a previous course in Şirince in 2014 on ultraproducts, and sometimes (4) my wish for improvement.

Contents

1 Monday, January 23, 2017

If there is a bijection from a set A to a set B, we shall write

$$A \approx B.$$

The relation $\approx$ is an **equivalence relation,** since

$$\begin{gathered} A \approx A, \\ A \approx B \implies B \approx A, \\ A \approx B \ \& \ B \approx C \implies A \approx C. \end{gathered}$$

In case $A \approx B$, we may say A and B are **equipollent.** We may also write

$$|A| = |B|\,;$$

but what does $|A|$ itself mean?

If A is a finite set, we normally let $|A|$ denote its size. Thus, defining

$$\mathbb{N} = \{1, 2, 3, \dots\} = \{x \in \mathbb{Z} \colon x > 0\},$$

the set of **counting numbers,** we have

$$\{x \in \mathbb{N} \colon x \mid 12\} = \{1, 2, 3, 4, 6, 12\},$$

so

$$\bigl|\{x \in \mathbb{N} \colon x \mid 12\}\bigr| = 6.$$

But in this case, what is 6? For our convenience, we shall define

$$6 = \{0, 1, 2, 3, 4, 5\},$$

a 6-element set.

What is $|A|$ if A is infinite? We define

$$\omega = \{0\} \cup \mathbb{N} = \{x \in \mathbb{Z} \colon x \geqslant 0\},$$

the set of **natural numbers.** Then $\mathbb{N} \approx \omega$ because of the bijection $x \mapsto x - 1$. We therefore define

$$|\mathbb{N}| = \omega.$$

A set is called **countable** if it is finite or equipollent with ω. But we shall see presently that there are uncountable sets.

Because equipollence is an equivalence relation, we may consider defining $|A|$ as the corresponding equivalence class,

$$\{X \colon X \approx A\}.$$

A problem with this is that the term *class* is actually appropriate here! if $A \neq \varnothing$, then $\{X \colon X \approx A\}$ is a **proper class,** namely a class that is not a set.

Every set is a class, but not every class is a set. Sets are collections that satisfy certain axioms: for us, the **Zermelo–Fraenkel axioms,** called **ZF,** along with the **Axiom of Choice,** called **AC.** Together, these axioms are denoted by **ZFC.** One of the axioms of ZF is

1 **Axiom** (Extension). *Sets that have the same elements that are sets are equal:*

$$\forall x \, \forall y \, \big(\forall z \, (z \in x \Leftrightarrow z \in y) \Rightarrow x = y\big).$$

All variables, here and in other formal expressions of set theory, refer to sets. In particular, sets A and B can be equal, even if A has an element that is not a set and that is not in B.

In this case though, our logic will still not distinguish between A and B. Briefly, we may assume that *all elements of sets are sets.*

This is a convenience for set theory. Elsewhere in mathematics, we do not usually consider elements of sets as sets. For example, in *point set topology,* which we shall look at later, the elements of sets are generally treated merely as points, which are not required to be sets themselves. However, in any particular application, these points can presumably be understood as certain sets.

Once we have sets, as governed by ZFC, then we can define collections of them by means of *formulas* that have single free variables. Such collections are **classes.** If $\varphi(x)$ is a singulary formula in the language of set theory, it defines the class denoted by

$$\{x\colon \varphi(x)\}.$$

For example, we can form the class

$$\Big\{x\colon \forall y\ \big(\forall z\ (z \in x \Leftrightarrow z \in y) \Rightarrow x = y\big)\Big\}.$$

By the Extension Axiom, this class is the **universal class,** called $\mathbf{V}$. Thus

$$\mathbf{V} = \{x\colon x = x\}.$$

Every set A is (or is equal to) the class $\{x\colon x \in A\}$. However, not every set is a class:

2 Theorem (Russell Paradox)**.** *The class $\{x\colon x \notin x\}$ is not a set.*

Proof. Suppose if possible that the class is the set A. Then

$$A \in A \implies A \notin A, \qquad\qquad A \notin A \implies A \in A,$$

which is absurd. $\square$

The proof requires A to be a set, since the variable x used in the definition of $\{x\colon x \notin x\}$ can be replaced only by sets.

It follows from the theorem that $\mathbf{V}$ itself is not a class, because of the following.

3 Axiom (Separation)**.** *Every subclass of a set is a set, that is, for every singulary formula $\varphi(x)$,*

$$\forall y\ \exists z\ \forall x\ \bigl(x \in z \Leftrightarrow x \in y \land \varphi(x)\bigr).$$

The subset $\{x\colon x \in A \land \varphi(x)\}$ of A is usually written as

$$\{x \in A\colon \varphi(x)\}.$$

We shall denote classes by boldface letters. These will be constants, not variables. If $\boldsymbol{C}$ is a class, then by definition

$$\begin{aligned}\mathscr{P}(\boldsymbol{C}) &= \bigl\{x\colon \forall y\ (y \in x \Rightarrow x \in \boldsymbol{C})\bigr\}\\ &= \{x\colon x \subseteq \boldsymbol{C}\}.\end{aligned}$$

This is the **power class** of $\boldsymbol{C}$. Here $\boldsymbol{C}$ may be a proper class; but in this case it does not belong to $\mathscr{P}(\boldsymbol{C})$, because the elements of this class (as of every class) are sets. A proper class is never an element of a class (much less a set).

4 Axiom (Power Set)**.** *The power class of a set is a set, which we shall call the* ***power set*** *of the set:*

$$\forall x\ \exists y\ \forall z\ (z \in y \Leftrightarrow z \subseteq x).$$

Note that

$$\mathbf{V} = \mathscr{P}(\mathbf{V}).$$

Thus $\mathbf{V} \approx \mathscr{P}(\mathbf{V})$, except that, strictly speaking we did not define the relation $\approx$ to exist between proper classes.

5 Theorem (Cantor). *For all sets A,*

$$A \not\approx \mathscr{P}(A).$$

Proof. We use the idea of the proof of the Russell Paradox. Supposing f to be an injection from A to $\mathscr{P}(A)$, we define

$$B = \{x \in A \colon x \notin f(x)\},$$

a subset of A. Then for all c in A,

$$c \in B \implies c \notin f(c), \qquad c \notin B \implies c \in f(c).$$

In either case, $B \neq f(c)$, because the two sets have different elements. Indeed, it is usually a logical axiom that equal things have all of the same properties, and in particular the converse of the Extension Axiom,

$$\forall y\ \forall z\ \bigl(y = z \Rightarrow \forall x\ (x \in y \Leftrightarrow x \in z)\bigr), \tag{1.1}$$

is true, and more generally, for all binary formulas $\varphi(x, y)$,

$$\forall y\ \forall z\ \Bigl(y = z \Rightarrow \forall x\ \bigl(\varphi(x, y) \Leftrightarrow \varphi(x, z)\bigr)\Bigr). \tag{1.2}$$

However, in an early paper, Abraham Robinson (called then Robinsohn) showed that one could *define* equality of sets by what we have called the Extension Axiom. This means one also has (1.1) by definition; and then, in order to obtain the generalization (1.2), one can use, as an axiom, the special case

$$\forall y\ \forall z\ \bigl(y = z \Rightarrow \forall x\ (y \in x \Leftrightarrow z \in x)\bigr).$$

In any case, at present we have $B \notin f[A]$, where by definition

$$f[A] = \{f(x) \colon x \in A\}.$$

so f is not surjective. □

The term *power set* can be understood as follows. First of all, for any sets A and B, we define B^A as the set of functions from A to B. By the ZF axioms, this is really a set. For, a function is a class of ordered pairs with certain properties, and an ordered pair can be defined as a certain set; if the domain of the function is a set, then the function itself is a set.*

For each n in ω, we understand

$$n = \{0, \dots, n-1\} = \{x \in \omega \colon x < n\}.$$

Then

$$0 = \varnothing, \qquad 1 = \{0\}, \qquad 2 = \{0, 1\},$$

and also

$$n + 1 = n \cup \{n\}.$$

Then by definition $2^A = \big\{\text{functions from } A \text{ to } \{0,1\}\big\}$, and so

$$2^A \approx \mathscr{P}(A),$$

because the function that assigns, to every f in 2^A, the subset $\{x \in A \colon f(x) = 1\}$ of A is a bijection with $\mathscr{P}(A)$.

We are going to show $\mathscr{P}(\omega) \approx \mathbb{R}$. First we shall define an injection from $\mathscr{P}(\omega)$ to $\mathbb{R}$. As a first attempt, if $A \subseteq \omega$, we define

$$f(A) = \sum_{k \in A} \frac{1}{2^{k+1}}. \tag{1.3}$$

Then $f(\varnothing) = 0$ and $f(\omega) = 1$, and in general

$$f(A) \in [0, 1].$$

---

*To be precise, (a, b) can be defined as the set $\big\{\{a\}, \{a, b\}\big\}$; and a function whose domain is a set is a set by the **Replacement Axiom.**

We have

$$f(\{2x\colon x \in \omega\}) = \frac{2}{3}, \qquad f(\{2x+1\colon x \in \omega\}) = \frac{1}{3}.$$

However, the equation $f(X) = 1/2$ has two solutions, $\{0\}$ and $\omega \smallsetminus \{0\}$; so f is not injective. We now define

$$g(A) = \sum_{k \in A} \frac{2}{3^{k+1}}. \tag{1.4}$$

By definition, $g[\mathscr{P}(\omega)]$ is the **Cantor set.** We shall show tomorrow that g is injective.

2 Tuesday, January 24, 2017

Suppose A and B are distinct subsets of ω. Defining

$$A \bigtriangleup B = (A \smallsetminus B) \cup (B \smallsetminus A),$$

the **symmetric difference** of A and B, we let

$$m = \min(A \bigtriangleup B).$$

We may assume $m \in B \smallsetminus A$. Then

$$\begin{aligned} A &\subseteq \{x \in A \colon x < m\} \cup \{x \in \omega \colon x > m\}, \\ B &\supseteq \{x \in A \colon x < m\} \cup \{m\}. \end{aligned}$$

With g as in (1.4), and letting $c = g\big(\{x \in A \colon x < m\}\big)$, we have

$$g(A) \leqslant c + \frac{1}{3^{m+1}} < c + \frac{2}{3^{m+1}} \leqslant g(B).$$

Thus g is injective.

Whenever an injective function exists from an arbitrary set A to an arbitary set B, we write

$$A \preccurlyeq B.$$

With g, we have shown $\mathscr{P}(\omega) \preccurlyeq \mathbb{R}$, in fact $\mathscr{P}(\omega) \preccurlyeq [0,1]$. We now show

$$[0,1) \preccurlyeq \mathscr{P}(\omega)$$

by defining an injective function h from $[0,1)$ to $\mathscr{P}(\omega)$. If f is as defined on $\mathscr{P}(\omega)$ by (1.3), then f is surjective onto $[0,1]$. In this case, we can let h be a right inverse of f, so that

$$f\bigl(h(y)\bigr) = y$$

for all y in $[0,1)$. This means that, for any such y, for some X in $\mathscr{P}(\omega)$,

$$f(X) = y, \qquad\qquad h(y) = X.$$

Since there are infinitely many values of y for which X is not uniquely determined, we have appealed to the **Axiom of Choice,** strictly speaking. This is needed when one has to make infinitely many choices, all at once. However, in the present case, we can make an explicit definition of h once for all, without needing AC. If $a \in [0,1)$, we define

$$h(a) = \{k \in \omega \colon a_k = 1\},$$

where the a_k are defined recursively by

$$a_k = \begin{cases} 0, & \text{if } a < \sum_{i<k} a_i/2^{i+1} + 1/2^{k+1}, \\ 1, & \text{if } a \geqslant \sum_{i<k} a_i/2^{i+1} + 1/2^{k+1}. \end{cases}$$

This ensures that, as desired,

$$a = \sum_{k=0}^{\infty} \frac{a_k}{2^{k+1}} = f\bigl(h(a)\bigr).$$

We have defined the a_n so that, for all k in ω, for some n in ω, we have $k \leqslant n$ and $a_n = 0$.

We now have

$$[0,1) \preccurlyeq \mathscr{P}(\omega) \preccurlyeq [0,1] \preccurlyeq \mathbb{R}.$$

Moreover, $\mathbb{R} \approx (0,1)$ because the function

$$x \mapsto \frac{x - 1/2}{x \cdot (1-x)}$$

is a bijection from $(0,1)$ to $\mathbb{R}$; its inverse can be computed as

$$y \mapsto \begin{cases} \dfrac{1}{2} + \dfrac{1}{2} \cdot \dfrac{\sqrt{1+y^2} - 1}{y}, & \text{if } y \neq 0, \\ \dfrac{1}{2}, & \text{if } y = 0. \end{cases}$$

Since $(0,1) \preccurlyeq [0,1)$, we obtain $\mathscr{P}(\omega) \approx \mathbb{R}$ from the following.

6 Theorem (Cantor–Schröder–Bernstein)**.** *If $A \preccurlyeq B$ and $B \preccurlyeq A$, then*

$$A \approx B.$$

Proof. Suppose f is an injection from A to B; and g, from B to A. By recursion, we define

$$\begin{aligned} A_0 &= A \smallsetminus g[B], & B_0 &= B \smallsetminus f[A], \\ A_{n+1} &= g[B_n], & B_{n+1} &= f[A_n]. \end{aligned}$$

By induction, for all n in $\mathbb{N}$, whenever $i < j \leqslant n$,

$$A_i \cap A_j = \varnothing, \qquad B_i \cap B_j = \varnothing.$$

Then also, by induction,

$$A_{2n} \cup A_{2n+1} \approx B_{2n} \cup B_{2n+1}.$$

Thus

$$\bigcup_{n \in \omega} A_n \approx \bigcup_{n \in \omega} B_n.$$

Finally,

$$A \smallsetminus \bigcup_{n\in\omega} A_n \approx B \smallsetminus \bigcup_{n\in\omega} B_n,$$

since

$$\begin{aligned} f\left[A \smallsetminus \bigcup_{n\in\omega} A_n\right] &= \bigcap_{n\in\omega} f\left[A \smallsetminus \bigcup_{k<n} A_k\right] \\ &= \bigcap_{n\in\omega}\left(B \smallsetminus \bigcup_{k\leqslant n} B_k\right) = B \smallsetminus \bigcup_{n\in\omega} B_n. \qquad \square \end{aligned}$$

Thus $\mathbb{R}$ is uncountable. Letting C be the Cantor set, namely the image of $\mathscr{P}(\omega)$ under g as defined in (1.4), we have also

$$C \approx \mathbb{R}.$$

In particular, C is uncountable (though we already knew this, because $C \approx \mathscr{P}(\omega)$).

3 Wednesday, January 25, 2017

The Cantor set (strictly the **Cantor ternary set**) C consists of the numbers in $[0,1]$ whose **ternary expansions** can be written without the digit 1. If $a \in [0,1]$, the ternary expansion of a is

$$0.a_0a_1a_2\cdots$$

where

$$a_k \in \{0,1,2\}, \qquad\qquad \sum_{k\in\omega}\frac{a_k}{3^{k+1}} = a.$$

Note that

$$0.a_0\cdots a_{n-1}1 = 0.a_0\cdots a_{n-1}0\overline{2},$$

so this is in C if $\{a_0,\dots,a_{n-1}\} \subseteq \{0,2\}$; but if

$$0.a_0\cdots a_{n-1}1 < x < 0.a_0\cdots a_{n-1}2,$$

then $x \notin C$. Some elements of C are shown in Figure 3.1. We have

$$C = \bigcap_{k\in\omega} F_k,$$

where

$$\begin{aligned} F_0 &= [0,1] \smallsetminus (1/3, 2/3), \\ F_{n+1} &= F_n \smallsetminus \bigcup\bigl\{(0.x_0\cdots x_n1, 0.x_0\cdots x_n2)\colon x_k \in \{0,2\}\bigr\}. \end{aligned}$$

Each set F_k is the union of finitely many closed intervals. Every intersection of a family of finite unions of closed intervals

ω	1
$\{0,1,2\}$	0.222
$\omega \setminus \{2\}$	0.221
$\{0,1\}$	0.22
$\omega \setminus \{1\}$	0.21
$\{0,2\}$	0.202
$\omega \setminus \{1,2\}$	0.201
$\{0\}$	0.2
X	$\displaystyle\sum_{k \in X} \frac{2}{3^{k+1}}$
$\omega \setminus \{0\}$	0.1
$\{1,2\}$	0.022
$\omega \setminus \{0,2\}$	0.021
$\{1\}$	0.02
$\omega \setminus \{0,1\}$	0.01
$\{2\}$	0.002
$\omega \setminus \{0,1,2\}$	0.001
$\varnothing$	0

Figure 3.1: The Cantor set

is called a **closed** subset of $\mathbb{R}$. Thus C is a closed subset of $\mathbb{R}$. The complement of a closed set is called **open.** The only subsets of $\mathbb{R}$ that are both closed and open are $\varnothing$ and $\mathbb{R}$.

The intersection of an open subset of $\mathbb{R}$ with C is called open in C; it might not be open in $\mathbb{R}$ (in fact it will not be). The intersection of a closed subset of $\mathbb{R}$ with C is called closed in C, but it is still closed in $\mathbb{R}$ anyway. However, C will have many subsets that are both open and closed in C.

A collection of subsets of $\mathbb{R}$ whose every finite subcollection has nonempty intersection is said to have the **finite intersection property** or **FIP.** In topological terms, the following theorem is that every closed bounded subset of $\mathbb{R}$ is **compact.** In fact the same is true in $\mathbb{R}^n$, though we shall not prove this (or use it).

7 Theorem (Heine–Borel)**.** *Every collection of bounded closed subsets of* $\mathbb{R}$ *with the finite intersection property has nonempty intersection.*

Proof. Let $\mathscr{F}$ be as in the hypothesis. We may assume that all elements of $\mathscr{F}$ are subsets of $[0,1]$. One of the collections $\mathscr{F} \cup \{[0,1/2]\}$ and $\mathscr{F} \cup \{[1/2,1]\}$ must have the FIP. For, suppose the first does not. Then for some finite subset $\mathscr{F}_0$ of $\mathscr{F}$, every element of $\bigcap \mathscr{F}_0$ must belong to $[1/2,1]$. Let $\mathscr{F}_1$ be any finite subset of $\mathscr{F}$. Then $\bigcap \mathscr{F}_0 \cap \bigcap \mathscr{F}_1$ is nonempty, and its every element belongs to $[1/2,1]$. Thus $\mathscr{F} \cup \{[1/2,1]\}$ has the FIP.

By recursion and induction, we obtain a sequence $(I_k \colon k \in \omega)$ of closed intervals such that $\mathscr{F} \cup \{I_k \colon k < n\}$ always has the FIP, and

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots,$$

and the length of I_k is $1/2^k$. If we let

$$a_k = \sup(I_k), \qquad b = \inf\{a_k \colon k \in \omega\},$$

then

$$\bigcap_{k\in\omega} I_k = \{b\}$$

(this is an exercise, but the proof will involve an observation to be made on Saturday: closed sets contain their *limit points*). Then $b \in \bigcap \mathscr{F}$. For, let $\varepsilon > 0$. For some n, we have $1/2^n < \varepsilon$, so

$$I_k \subseteq (b - \varepsilon, b + \varepsilon).$$

For every F in $\mathscr{F}$, since $F \cap I_k \neq \varnothing$, the set F has an element in $(b - \varepsilon, b + \varepsilon)$. This being so for all positive ε, and F being closed, we have $b \in F$ (again because closed sets contain their limit points). $\square$

In particular, C is compact. Using the bijection g from $\mathscr{P}(\omega)$ to C, we can define the closed subsets of $\mathscr{P}(\omega)$ as $g^{-1}[X]$, where X is a closed subset of C. However, we shall first give an independent definition of the closed subsets of $\mathscr{P}(\omega)$ and prove a theorem analogous to Heine–Borel.

4 Thursday, January 26, 2017

Starting with a collection $\{P_k\colon k \in \omega\}$ of **(propositional) variable,** we define **(propositional) formulas** recursively:

1. Each variable is a formula, namely an **atomic** formula.
2. If F is a formula, then so is $\neg G$, the **negation** of F.
3. If F and G are formulas, then so is $(F \wedge G)$, the **conjunction** of F and G.

8 Theorem. *Every formula is **uniquely readable:***

1. *No atomic formula is also a negation or a conjunction.*
2. *No negation is also a conjunction.*
3. *Every conjunction is uniquely so.*

Proof. Only the last claim is not entirely clear. By induction, we show that for all formulas F,
(a) no proper initial segment of F is a formula, and
(b) F is not a proper initial segment of any formula.
1. The claim is clearly true when F is atomic.
2. Suppose the claim is true when F is a formula G. Then the claim must be true when F is $\neg G$. For if H is a proper initial segment of $\neg G$, then H is of the form $\neg K$ for some K, which is a proper initial segment of G, so, by hypothesis, K cannot be a formula, and therefore H cannot be a formula. There is a similar argument if $\neg G$ is a proper initial segment of H.

3. Similarly, if the claim is true when F is G or H, then it must be true when F is $(G \wedge H)$.

By induction, which is made possible by the recursive definition of formulas, the claim holds for all formulas F. $\square$

The foregoing theorem allows us to make recursive definitions of functions on the set of all formulas. For example, for all subsets A of ω, we recursively define which formulas are **true** in A. We shall express that a formula F is true in A by writing

$$A \vDash F.$$

Then by definition

(1) $A \vDash P_k \iff k \in A$;

(2) $A \vDash \neg F \iff A \nvDash F$;

(3) $A \vDash (F \wedge G) \iff A \vDash F \;\;\&\;\; A \vDash G$.

Note that the expressions $\iff$ and & here are just abbreviations of ordinary language. Without recursion, we define

$$\mathrm{Mod}(F) = \{X \subseteq \omega \colon X \vDash F\}.$$

If Γ is a set of formulas, we define

$$\mathrm{Mod}(\Gamma) = \bigcap\{\mathrm{Mod}(F) \colon F \in \Gamma\};$$

this is the set of **models** of Γ. If every finite subset of Γ has a model, we shall say that Γ is **consistent.** We shall show that every consistent set of formulas has a model. To do this, we make one more recursive definition.

(1) $V(P_k) = \{k\}$.

(2) $V(\neg F) = V(F)$.

(3) $V\big((F \land G)\big) = V(F) \cup V(G)$.

We do not really need recursion here: we can just say

$$V(F) = \{k \in \omega \colon P_k \text{ occurs in } F\}.$$

9 Theorem. *For all formulas F, for all subsets A and B of ω, if*

$$V(F) \cap A = V(F) \cap B,$$

then

$$A \vDash F \iff B \vDash F.$$

Proof. Induction. $\square$

10 Theorem (Compactness for propositional logic)**.** *Every consistent set of propositional formulas has a model.*

Proof. Let Γ be a consistent set of formulas. Just as in the proof of the Heine–Borel Theorem, one of $\Gamma \cup \{P_0\}$ and $\Gamma \cup \{\neg P_0\}$ must be consistent. In this way, by recursion, we obtain a sequence $(G_k \colon k \in \omega)$, where each G_k is either P_k or $\neg P_k$, and each collection $\Gamma \cup \{G_k \colon k < n\}$ is consistent. Let

$$A = \{k \in \omega \colon G_k \text{ is } P_k\}.$$

For all F in Γ, the collection

$$\{F\} \cup \{G_k \colon k \in V(F)\}$$

has a model B. Then for all k in $V(F)$, we have $B \vDash G_k$, and so

$$k \in B \iff k \in A.$$

By the foregoing theorem, since $B \vDash F$, also $A \vDash F$. Thus $A \in \mathrm{Mod}(\Gamma)$. $\square$

5 Friday, January 27, 2017

If $\{F_i \colon i \in I\}$ is a family of subsets of $\mathbb{R}$, each being a finite union $I_0 \cup \cdots \cup I_{n-1}$ of closed intervals, then again, by definition, $\bigcap_{i \in I} F_i$ is a **closed subset** of $\mathbb{R}$. For any set Ω, since its collection of finite subsets is

$$\bigl\{X \in \mathscr{P}(\Omega) \colon\ |X| < \omega\bigr\},$$

we shall denote this collection by

$$\mathscr{P}_\omega(\Omega).$$

11 Theorem. *If $\mathscr{F}$ is the family of closed subsets of $\mathbb{R}$, then*

(1) $\mathscr{X} \in \mathscr{P}(\mathscr{F}) \implies \bigcap \mathscr{X} \in \mathscr{F}$*;*

(2) $\mathscr{Y} \in \mathscr{P}_\omega(\mathscr{F}) \implies \bigcup \mathscr{X} \in \mathscr{F}$*.*

Proof. 1. Since closed sets are already intersections, the first claim is clear.

2. We shall show by induction that, for all n in ω, for all n-element subsets $\mathscr{A}$ of $\mathscr{F}$, $\bigcup \mathscr{A} \in \mathscr{F}$. When $n = 0$, then $\bigcup \mathscr{A} = \bigcup \varnothing = \varnothing$, which belongs to $\mathscr{F}$ since, above, we can take one of the F_i to be the empty union. Suppose the claim holds when $n = m$, but now $\mathscr{A} = \{A_k \colon k \leqslant m\}$. By hypothesis, $\bigcup_{k<m} A_k \in \mathscr{F}$, so it is an intersection $\bigcap_{i \in I} F_i$ of finite unions of closed intervals. But A_m is a similar intersection

$\bigcap_{j\in J} G_j$. We now have

$$\begin{aligned}\bigcup \mathscr{A} = \bigcup_{k<m} A_k \cup A_m &= \bigcap_{i\in I} F_i \cup \bigcap_{j\in J} G_j\\ &= \bigcap_{i\in I}\left(F_i \cup \bigcap_{j\in J} G_j\right)\\ &= \bigcap_{i\in I}\bigcap_{j\in J}(F_i \cup G_j),\end{aligned}$$

which is in $\mathscr{F}$. □

Again, the complement of a closed set is called **open.** If τ is the family of open subsets of $\mathbb{R}$, then, with $\mathscr{F}$ as in the theorem,

$$\tau = \{\mathbb{R} \smallsetminus X \colon X \in \mathscr{F}\} = \{X^{\mathrm{c}} \colon X \in \mathscr{F}\},$$

and so

(1) $\mathscr{X} \in \mathscr{P}(\tau) \implies \bigcup \mathscr{X} \in \tau$;

(2) $\mathscr{Y} \in \mathscr{P}_\omega(\tau) \implies \bigcap \mathscr{X} \in \tau$; and this is equivalent to

  (a) $\mathbb{R} \in \tau$, and

  (b) $Y, Z \in \tau \implies Y \cap Z \in \tau$.

Precisely because τ meets these conditions, τ is called a **topology** on $\mathbb{R}$.

Let us denote by

$$L$$

the set of propositional formulas with variables from the set $\{P_k \colon k \in \omega\}$. Then the family $\{\mathrm{Mod}(\Gamma) \colon \Gamma \subseteq L\}$ satisfies the conditions to be closed. In particular

(a) $\varnothing = \mathrm{Mod}(P_0 \wedge \neg P_0)$, and

(b) $\mathrm{Mod}(F) \cup \mathrm{Mod}(G) = \mathrm{Mod}(F \vee G)$,

where $F \vee G$ means $\neg(\neg F \wedge \neg G)$.

If (A, τ) and (B, σ) are two topological spaces, $f\colon A \to B$, and

$$X \in \sigma \implies f^{-1}[X] \in \tau,$$

then f is called **continuous;** if also f is a bijection, and f^{-1} is continuous, then f is called a **homeomorphism.** If $C \subseteq A$, it is easy to show that $\{C \cap X \colon X \in \tau\}$ is a topology on C, called the **subspace topology.** We give the Cantor set this topology from $\mathbb{R}$.

12 Theorem. *The function g in* (1.4) *is a homeomorphism from $\mathscr{P}(\omega)$ to the Cantor set.*

Proof. Given n in $\mathbb{N}$ and a subset A of n, let us define the formula $F_{n,A}$ as

$$E_0 \wedge \cdots \wedge E_{n-1},$$

where

$$E_k \text{ is } \begin{cases} P_k, & \text{if } k \in A, \\ \neg P_k, & \text{if } k \in n \smallsetminus A. \end{cases}$$

Then

$$\mathrm{Mod}(F_{n,A}) = \{X \subseteq \omega \colon X \cap n = A\}.$$

For any F in L, there is n in $\mathbb{N}$ such that $V(F) \subseteq n$. Now let

$$I = \{X \subseteq n \colon X \vDash F\}.$$

Then

$$\mathrm{Mod}(F) = \bigcup_{X \in I} \{Y \subseteq \omega \colon Y \cap n = X\} = \bigcup_{X \in I} \mathrm{Mod}(F_{n,X}).$$

Since

$$\mathrm{Mod}(F)^{\mathrm{c}} = \mathrm{Mod}(\neg F),$$

we can conclude that the open subsets of L are just the unions of sets $\mathrm{Mod}(F_{n,A})$.

For all X in $\mathscr{P}(\omega)$,

$$X \vDash F_{n,A} \iff A \subseteq X \subseteq A \cup \{x \in \omega \colon x \geqslant n\}.$$

Thus

$$\begin{aligned} g[\mathrm{Mod}(F_{n,A})] &= C \cap \left[g(A), g(A) + \frac{1}{3^n}\right] \\ &= C \cap \left(g(A) - \frac{1}{3^n}, g(A) + \frac{2}{3^n}\right). \end{aligned}$$

This being open in C, g^{-1} is continuous.

For the continuity of g, we observe that the interval $(g(A) - 1/3^n, g(A) + 2/3^n)$ has length $1/3^{n-1}$. Let O be an open subset of $\mathbb{R}$ and $a \in C \cap O$. For some positive ε_a we have

$$(a - \varepsilon_a, a + \varepsilon_a) \subseteq O.$$

Now let n_a be large enough that $1/3^{n_a - 1} < \varepsilon_a$. For some subset A_a of n_a, we have

$$a \in \left(g(A_a) - \frac{1}{3^{n_a}}, g(A_a) + \frac{2}{3^{n_a}}\right),$$

but then also

$$\left(g(A_a) - \frac{1}{3^{n_a}}, g(A_a) + \frac{2}{3^{n_a}}\right) \subseteq (a - \varepsilon_a, a + \varepsilon_a).$$

Thus

$$C \cap O = \bigcup_{x \in C \cap O} g[\mathrm{Mod}(F_{n_x, A_x})],$$

so $g^{-1}[C \cap O] = \bigcup_{x \in C \cap O} \mathrm{Mod}(F_{n_x, A_x})$, and open set. □

6 Saturday, January 28, 2017

If A is a subset of a topological space, and $p \in A$, there are two possibilities.

1. If, for some open set O, we have $p \in O$ and $O \subseteq A$, then A is called a **neighborhood** of p, and p is an **interior point** of A.

2. If, for all open sets O that contain p, we have $O \cap A^c \neq \varnothing$, then p is a **limit point** of A^c. In this case p is also a limit point of $A^c \cup \{p\}$.

To prove the Heine–Borel Theorem (Theorem 7, page 17), we used the easy observation that every open set is a neighborhood of all of its points, so that every closed set must contain all of its limit points. The converse takes a little more work:

13 Theorem. *In a topological space, every set that is a neighborhood of all of its points is open, and every set that contains all of its limit points is closed.*

Proof. Exercise. ☐

A topological space (Ω, τ) is **compact** if any of the following equivalent conditions is satisfied:

1. Every family of closed sets whose every finite subfamily has nonempty intersection has nonempty intersection.

2. For every family of closed sets with empty intersection, there is a finite subfamily $\{F_i\colon i < n\}$ such that

$$F_0 \cap \cdots \cap F_{n-1} = \varnothing.$$

3. For every family $\mathscr{O}$ of open sets whose union is all of Ω, there is a finite subfamily $\{O_i\colon i < n\}$ such that

$$O_0 \cup \cdots \cup O_{n-1} = \Omega.$$

   Here $\mathcal{O}$ is called an **open covering** of Ω, and then $\{O_i\colon i < n\}$ may be referred to as a **finite sub-covering** of $\mathcal{O}$.

The Heine–Borel Theorem (our Theorem 7) is that every closed, bounded subset of $\mathbb{R}$ is compact. (Actually it is true for each $\mathbb{R}^n$.) With the Compactness Theorem for propositional logic (Theorem 10), we showed that $\mathscr{P}(\omega)$ is compact in the topology whose closed sets are just the sets $\operatorname{Mod}(\Gamma)$, where $\Gamma \subseteq L$, L being the set of propositional formulas in the variables P_k, where $k \in \omega$. Here, for each F in L,

$$\operatorname{Mod}(F)^{\mathrm{c}} = \operatorname{Mod}(\neg F),$$

so that $\operatorname{Mod}(F)$ is **clopen:** both closed and open.

14 Theorem. *In $\mathscr{P}(\omega)$, the clopen sets are precisely the sets $\operatorname{Mod}(F)$, where $F \in L$.*

Proof. Suppose $\operatorname{Mod}(\Gamma)$ is open (as well as closed) for some subset Γ of L. Then $\operatorname{Mod}(\Gamma)^{\mathrm{c}}$ is closed, so it is compact (as is every closed subset of a compact space, easily). But

$$\operatorname{Mod}(\Gamma)^{\mathrm{c}} = \bigcup_{F\in\Gamma} \operatorname{Mod}(\neg F).$$

By Compactness, there is a finite subset $\{F_k\colon k<n\}$ of Γ such that

$$\begin{gathered}\mathrm{Mod}(\Gamma)^{\mathrm{c}}=\mathrm{Mod}(\neg F_0)\cup\dots\cup\mathrm{Mod}(\neg F_{n-1}),\\ \mathrm{Mod}(\Gamma)=\mathrm{Mod}(F_0\wedge\dots\wedge F_{n-1}).\end{gathered}\qquad\square$$

The relation $\sim$ of **logical equivalence** on L is given by

$$F\sim G\iff\mathrm{Mod}(F)=\mathrm{Mod}(G).$$

We can now define

$$\begin{gathered}[F]=\{X\in L\colon X\sim F\},\\ L/{\sim}=\{[X]\colon X\in L\}.\end{gathered}$$

The definitions ensure that there is a well-defined injection $X\mapsto\mathrm{Mod}(X)$ from $L/{\sim}$ to $\mathscr{P}(\omega)$. By the last theorem, the map is also surjective onto the collection $\mathscr{B}$ of clopen subsets of ω. Here $\mathscr{B}$ is closed under

(1) the binary operations $\cap$ and $\cup$,

(2) the singulary operation $^{\mathrm{c}}$, and

(3) the nullary operations $\varnothing$ and ω (that is, $\mathscr{B}$ contains these sets).

This makes $\mathscr{B}$ a *Boolean subalgebra* of $\mathscr{P}(\omega)$. Since

$$\begin{gathered}\mathrm{Mod}(F\wedge G)=\mathrm{Mod}(F)\cap\mathrm{Mod}(G),\\ \mathrm{Mod}(F\vee G)=\mathrm{Mod}(F)\cup\mathrm{Mod}(G),\\ \mathrm{Mod}(\neg F)=\mathrm{Mod}(F)^{\mathrm{c}},\\ \mathrm{Mod}(P_0\wedge\neg P_0)=\varnothing,\\ \mathrm{Mod}(P_0\vee\neg P_0)=\omega,\end{gathered}$$

$L/\sim$ is a Boolean algebra with respect to the (well-defined) operations given by

$$\begin{aligned}
[F] \wedge [G] &= [F \wedge G], \\
[F] \vee [G] &= [F \vee G], \\
\neg[F] &= [\neg F], \\
\perp &= [P_0 \wedge \neg P_0], \\
\top &= [P_0 \vee \neg P_0].
\end{aligned}$$

In general, an abstract **Boolean algebra** (like $L/\sim$) is a set B with operations $\wedge$, $\vee$, $\neg$, $\perp$, and $\top$ with the following properties.

1. The binary operations $\vee$ and $\wedge$ are **commutative:**

$$x \vee y = y \vee x, \qquad x \wedge y = y \wedge x.$$

2. The elements $\perp$ and $\top$ are **identities** for $\vee$ and $\wedge$ respectively:

$$x \vee \perp = x, \qquad x \wedge \top = x.$$

3. $\vee$ and $\wedge$ are mutually **distributive:**

$$\begin{aligned}
x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z), \\
x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z).
\end{aligned}$$

4. The element $\neg x$ is a **complement** of x:

$$x \vee \neg x = \top, \qquad x \wedge \neg x = \perp.$$

Additional properties like associativity of $\wedge$ and $\vee$ follow from the given identities:

15 Theorem (E. Huntington, 1904). *In any Boolean algebra:*

$$\begin{aligned} x \vee x &= x, & x \wedge x &= x, \\ x \vee \top &= \top, & x \wedge \bot &= \bot, \\ x \vee (x \wedge y) &= x, & x \wedge (x \vee y) &= x, \end{aligned}$$

$$\neg\neg x = x,$$

$$\begin{aligned} \neg(x \vee y) &= \neg x \wedge \neg y, & \neg(x \wedge y) &= \neg x \vee \neg y, \\ (x \vee y) \vee z &= x \vee (y \vee z), & (x \wedge y) \wedge z &= x \wedge (y \wedge z). \end{aligned}$$

Proof. We give only an example:

$$x \vee (x \wedge y) = (x \wedge \top) \vee (x \wedge y) = x \wedge (\top \vee y) = x \wedge \top = x.$$

□

We shall investigate how $\mathscr{P}(\omega)$, or more precisely a space homeomorphic with it, can be obtained from the Boolean algebra $L/{\sim}$. The same construction will work for any Boolean algebra, and then the algebra can be recovered as being isomorphic to the algebra of clopen subsets of the space. (This is the Stone Representation Theorem.)

We shall need that, on any Boolean algebra, there is a partial ordering $\vdash$ given by

$$x \vdash y \iff x \wedge y = x.$$

Note that

$$x \wedge y = x \iff x \vee y = y.$$

We may henceforth blur the distinction between formulas in L and their equivalence classes in $L/{\sim}$. If $A \subseteq \omega$, we define

$$\mathrm{Th}(A) = \{X \in L \colon A \vDash X\}.$$

This is the **theory** of A, and it has the following properties.

1. If F and G are in $\mathrm{Th}(A)$, then $(F \wedge G) \in \mathrm{Th}(A)$.
2. If $F \in \mathrm{Th}(A)$ and $F \vdash G$, then $G \in \mathrm{Th}(A)$.
3. $F \notin \mathrm{Th}(A)$ if and only if $\neg F \in \mathrm{Th}(A)$.

By the first two properties, $\mathrm{Th}(A)$ is a **filter** of the algebra $L/{\sim}$; then the third property makes $\mathrm{Th}(A)$ an **ultrafilter,** that is, a maximal filter (the whole algebra not being counted as a filter; any larger filter than $\mathrm{Th}(A)$ would contain some F not in $\mathrm{Th}(A)$; but then $\mathrm{Th}(A)$ contains $\neg F$, so the larger filter contains $F \wedge \neg F$, which is equivalent to $\perp$, and $\perp \vdash G$ for all G in L). The converse also holds:

16 Theorem. *Every ultrafilter of $L/{\sim}$ is the theory of some element of $\mathscr{P}(\omega)$.*

Proof. Given an ultrafilter Φ of $L/{\sim}$, we may let

$$A = \{k \in \omega \colon P_k \in \Phi\}.$$

By induction $U = \mathrm{Th}(A)$, that is, for all F in L,

$$F \in U \iff A \vDash F. \qquad \square$$

For any Boolean algebra B, we shall denote the set of ultrafilters of B by

$$\mathrm{S}(B);$$

this is the **Stone space** of B, because it will have a topology. In our case, we have a bijection $X \mapsto \mathrm{Th}(X)$ from $\mathscr{P}(\omega)$ to $\mathrm{S}(L/{\sim})$, and this will be a homeomorphism.

7 Sunday, January 29, 2017

We have been working with the relation $\vDash$ from $\mathscr{P}(\omega)$ to L. We have used it to define $X \mapsto \mathrm{Mod}(X)$ from L to $\mathscr{P}(\mathscr{P}(\omega))$, where

$$\mathrm{Mod}(F) = \{Y \in \mathscr{P}(\omega) \colon Y \vDash F\}.$$

Here

$$\mathrm{Mod}(F \wedge G) = \mathrm{Mod}(F) \cap \mathrm{Mod}(G),$$
$$\mathrm{Mod}(\neg F) = \mathrm{Mod}(F)^{\mathrm{c}},$$

so that, when we define

$$F \sim G \iff \mathrm{Mod}(F) = \mathrm{Mod}(G),$$

the map $X \mapsto \mathrm{Mod}(X)$ induces a Boolean-algebra embedding of $L/{\sim}$ in $\mathscr{P}(\mathscr{P}(\omega))$. As we have shown (Theorem 14, page 27), the embedding is an isomorphism with the algebra of clopen subsets of $\mathscr{P}(\omega)$.

We have also defined a "dual" map, $Y \mapsto \mathrm{Th}(Y)$, from $\mathscr{P}(\omega)$ to $\mathscr{P}(L/{\sim})$, where

$$\mathrm{Th}(A) = \{X \in L \colon A \vDash X\};$$

by Theorem 16 (page 31), the map is a bijection onto $\mathrm{S}(L/{\sim})$, the set of ultrafilters of $L/{\sim}$.

We have already defined

$$\mathrm{Mod}(\Gamma) = \bigcap_{X \in \Gamma} \mathrm{Mod}(X)$$

when $\Gamma \subseteq L$; likewise we can define

$$\mathrm{Th}(\mathscr{A}) = \bigcap_{Y \in \mathscr{A}} \mathrm{Th}(Y)$$

when $\mathscr{A} \subseteq \mathscr{P}(\omega)$. Then

$$\Gamma \subseteq \Delta \implies \mathrm{Mod}(\Gamma) \supseteq \mathrm{Mod}(\Delta),$$
$$\mathscr{A} \subseteq \mathscr{B} \implies \mathrm{Th}(\mathscr{A}) \supseteq \mathrm{Th}(\mathscr{B}).$$

Simply on this basis,

$$\mathrm{Mod} \circ \mathrm{Th} \circ \mathrm{Mod} = \mathrm{Mod},$$
$$\mathrm{Th} \circ \mathrm{Mod} \circ \mathrm{Th} = \mathrm{Th},$$

so that there is a one-to-one correspondence, called a **Galois correspondence,** between the sets $\mathrm{Mod}(\Gamma)$ and the sets $\mathrm{Th}(\mathscr{A})$. In the original Galois theory, the correspondence is between subfields of a field K and subgroups of the group of automorphisms of K; one obtains this by using, in place of our $\vDash$, the relation R from the field to the automorphism group given by

$$x \mathrel{R} \sigma \iff x^{\sigma} = x.$$

In our case, the sets $\mathrm{Th}(\mathscr{A})$ are filters of $L/{\sim}$, while the sets $\mathrm{Mod}(\Gamma)$ can be called **elementary classes** (though all this means is that they are the classes of models of sets of formulas).

17 Theorem (Stone Representation)**.** *Every Boolean algebra embeds in an algebra $\mathscr{P}(\Omega)$ for some set Ω.*

Proof. If we replace L with an arbitrary Boolean algebra B, then we can also replace $\mathscr{P}(\omega)$ with $\mathrm{S}(B)$, and $\vDash$ with $\in$. When we define the map $x \mapsto [x]$ from B to $\mathscr{P}(\mathrm{S}(B))$ by

$$[a] = \{U \in \mathrm{S}(B) \colon a \in U\},$$

then

$$[a] \cap [b] = [a \wedge b],$$
$$[a]^{\mathrm{c}} = [\neg a],$$

so the map is a homomorphism of Boolean algebras. It is an embedding, by the Axiom of Choice, or rather by the weaker axiom called the **Prime Ideal Theorem** (which is that every proper ideal of a ring is included in a prime ideal; the Axiom of Choice gives that every proper ideal is included in a maximal ideal; maximal ideals are always prime, but in Boolean rings, prime ideals are also maximal). □

In the proof, the subsets $[a]$ of $\mathrm{S}(B)$ serve as the clopen sets of a topology, the **Stone topology;** the closed sets are

$$\bigcap_{x \in I} [x],$$

where $I \subseteq B$. This topology is always compact: showing this comes down to observing that if $\bigcap_{x \in I_0} [x]$ is never empty when I_0 is a finite subset of I, then I is included in a proper filter, and therefore (by the Prime Ideal Theorem) an ultrafilter U; but this just means $U \in \bigcap_{x \in I} [x]$.

A **first-order logic,** such as the logic of set theory, defines formulas as in propositional logic, except that the atomic formulas are not propositional variables, but (in the case of set theory) formulas $x \in y$; also, if φ is a formula, and x is a variable, then so is $\exists x\ \varphi$. One has the notion of a **free variable** of a formula; if a formula has no free variable, the formula is a **sentence.** Every sentence has a class of **models,** which, considered in themselves, are **structures.** Defining logical equivalence as before, one obtains a Boolean algebra of sentences, called a **Lindenbaum algebra** after a student of Tarski, murdered by the Nazis. The Stone space of this algebra is automatically compact. The Compactness Theorem can then be understood as being that every ultrafilter of the Lindenbaum algebra is in fact the theory of some structure.

Finally, in the Stone Representation Theorem, instead of a Boolean algebra, we may start with an arbitrary topological space and extract its algebra of clopen subsets. However, the Stone space of this algebra will not be homeomorphic with the original space unless this is compact and **totally disconnected** (for any two points, some clopen set contains only one of them).