Closure, induction, and numbers

Professor Cian Dorr

15th September 2022

New York University

Closed sets (recap)

Suppose R is a relation on A and $X \subseteq A$.

Definition

X is *closed under* R := for all $x, y \in A$, if $x \in X$ and Rxy, then $y \in X$.

Intuitively: if you start inside X, you can't "escape" by taking an R-step.

Obvious Fact about Intersection

If X and Y are both closed under R, then $X \cap Y$ is closed under R.

Proof: Suppose X and Y are closed under R; $z \in X \cap Y$; and Rzu. Then $u \in X$ since $z \in X$ and X is closed under R, and $u \in Y$ since $z \in Y$ and Y is closed under R. Hence $u \in X \cap Y$.

Closed under a relation from A^2 to A

We extend the concept of closedness from *relations on* A to *relations from* $A^2 (= A \times A)$ *to* A:

Definition

Where R is a relation from $A \times A$ to A and $X \subseteq A$, X is *closed under* R iff for all $x, y, z \in A$, if $x \in X$ and $y \in X$ and $R\langle x, y\rangle z$, then $z \in X$.

We can extend this definition in the obvious way to relations from $A^3 (= (A \times A) \times A$, $A^4 (= ((A \times A) \times A) \times A$, etc. to $A. \dots$

Intuitively: The elements of X can't be put together into a tuple from which we could take an R-step to the outside of X.

- The Obvious Fact about Intersections also applies to this kind of R, by the same reasoning as before.

Closed under a relation from $\mathcal{P}A$ to A

The concept can also be extended to relations from the *powerset* of a set to the set, i.e. relations that subsets of A can bear to elements of A.

Definition

Where R is a relation from $\mathcal{P}A$ to A and $X \subseteq A$, X is *closed under* R iff for all $Y \subseteq X$ and $z \in A$, if RYz, then $z \in X$.

- The Obvious Fact about Intersections also applies to this kind of R, by the same reasoning as before.

Closed under a family of relations

Sometimes we are interested in some family of relations $R_1, \dots, R_n$, where each one is either from A to A or from A^2 to A or from A^3 to $A \dots$, or perhaps from $\mathcal{P}A$ to A. We say that a set X is closed under this family of relations iff X is closed under every member of the family.

- The Obvious Fact about Intersection applies by the same reasoning as before: i.e., the intersection of two sets both closed under $R_1, \dots, R_n$ is itself closed under $R_1, \dots, R_n$.

Some more definitions

Suppose $V \subseteq \mathcal{P}A$. Then:

Definition

$\bigcap V$ (the intersection of V) $:= \{y \in A \mid y \in X \text{ for all } X \in V\}$.

Definition

$\bigcup \mathbf{V}$ (the union of $\mathbf{V}$) $:= \{y \in A \mid y \in X \text{ for some } X \in \mathbf{V}\}$.

(Don't confuse these big symbols with the small $\cap$ and $\cup$, which are binary operators.)

We can understand $\bigcap$ and $\bigcup$ here as *functions from $\mathcal{PP}A$ to $\mathcal{P}A$*.

So, it makes sense to ask whether some set $\mathbf{V} \subseteq \mathcal{P}A$ is closed under intersection or union. $\mathbf{V}$ is closed under intersection iff whenever $\mathbf{W} \subseteq V$, $\bigcap \mathbf{W} \in V$.

The “smallest” set with a certain property

Now, suppose that $\mathbf{V} \subseteq \mathcal{P}A$ is closed under intersection.

Then since $\mathbf{V} \subseteq \mathbf{V}$, we must have $\bigcap \mathbf{V} \in \mathbf{V}$.

Since $\bigcap \mathbf{V} \subseteq X$ for all $X \in \mathbf{V}$, it’s often called the “smallest” element of $\mathbf{V}$.

- N.B. this idiomatic use of “smallest” has nothing to do with our cardinality-theoretic definition of “at least as big as”!

The closure of a set under a relation

Fact

When R is a relation on A, the set of subsets of A that are closed under R is closed under intersection.

Proof: Suppose that every $X \in \mathbf{V}$ is closed under R. To show that $\bigcap \mathbf{V}$ is also closed under R, suppose that $x \in \bigcap \mathbf{V}$ and Rxy. Then for every $X \in \mathbf{V}$, $y \in X$ (since X is closed under R). Hence, $y \in \bigcap \mathbf{V}$.

Fact

For any $B \subseteq A$, the set of all sets $X \subseteq A$ such that $B \subseteq X$ is closd under intersection.

Proof: Suppose that $Y \subseteq X$ for every $X \in \mathbf{V}$; we need to show that $Y \subseteq \bigcap \mathbf{V}$. So, suppose $x \in Y$. Then $x \in X$ for every $X \in \mathbf{V}$ by assumption. So, $x \in \bigcap \mathbf{V}$.

So by the Obvious Fact about Intersections, we can derive that the intersection of these two sets is also closed under intersection, i.e.:

The closure of a set under a relation

Definition

Where R is a relation on A and $B \subseteq A$, the *closure of* B *under* R is the smallest subset of A that is a superset of B and is closed under R. That is:

$$\bigcap\{X \subseteq A \mid B \subseteq X \text{ and } X \text{ is closed under } R\}$$

It follows from the previous facts that the closure of B under R (i) is a superset of X; (ii) is closed under R; and (iii) is a subset of any other set X with properties (i) and (ii).

- All of the above carries over to relations from A^2 to A; to relations from A^3 to A; to relations from $\mathcal{P}A$ to A; and to families of relations of these different types.

Examples

-

Proof by induction

Suppose R is a relation on A, $B \subseteq A$, and C is the closure of B under R, and we would like to prove that every member of C has a certain property ϕ.

Then we can do so by proving the following two things:

1. Every element of B has property ϕ.
2. ϕ is preserved by R: i.e., if x has ϕ and Rxy, then y has ϕ.

This is called a *proof by induction*. Part 1 is called the *base case*; part 2 is called the *induction step*.

Why does this work? Well, consider the set $\{x \in A \mid \phi(x)\}$. By (i) it is a superset of B; by (ii) it is closed under R. So it's a superset of C. In other words, every member of C is ϕ.

Finite subsets, defined

Here's a nice example. Consider some set A, and define the relation AddOne on $\mathcal{P}A$ as

$$\{\langle X, Y\rangle | Y = X \cup \langle z\rangle \text{ for some } z \in A \setminus X\}$$

We define $\mathcal{P}_{\text{fin}}A$ (the set of *finite subsets* of A) to be the closure of $\{\varnothing\}$ under AddOne.

- N.B. that's $\{\varnothing\}$, not $\varnothing$—the closure of $\varnothing$ under any relation is just $\varnothing$!

We can then define "*A is finite*" to mean $A \in \mathcal{P}_{fin}A$. "*A is infinite*" to mean *A is not finite*.

- This gives an alternative to Dedekind's definition. Recall that a Dedekind-infinite set is one on which there is an injection that isn't a surjection; a Dedekind-finite set is a set that isn't Dedekind-infinite.

A proof by induction

Let's prove that whenever $X \in \mathcal{P}_{\mathsf{fin}} A$, X is Dedekind-finite.

We need to prove the following:

1. Base case: every member of $\{\varnothing\}$ is Dedekind-finite; in other words, $\varnothing$ is Dedekind-finite.
2. Induction step: if $\mathsf{AddOne} X Y$ and X is Dedekind-finite, then Y is Dedekind-finite.

For the base case, it suffices to note that there is only one relation on $\varnothing$, namely $\varnothing$, which is a bijection.

A proof by induction (continued)

For the induction step, suppose that $\mathrm{AddOne}\,XY$, i.e. $Y = X \cup \{z\}$ where $z \notin X$. We need to show that if X is Dedekind-finite, Y is Dedekind-finite; or equivalently, that if Y is Dedekind-infinite, X is also Dedekind-infinite.

This follows from the following three facts.

Fact 1: if two sets are equinumerous, then if one is Dedekind-infinite so is the other.

Fact 2: if z and u are both elements of some set Y, then $Y \setminus \{z\}$ and $Y \setminus \{u\}$ are equinumerous.

Fact 3: if some set Y is Dedekind-infinite, then there exists $u \in Y$ such that $Y \setminus \{u\}$ is Dedekind-infinite.

For fact 3, it suffices to note that if $f : Y \to Y$ is injective and $u \notin \mathrm{range}\, f$, then the restriction of f to $Y \setminus \{u\}$ (i.e., $f \setminus \{\langle u, fu\rangle\}$) is an injection $Y \setminus \{u\} \to Y \setminus \{u\}$ whose range does not include fu.

The natural numbers

Peano's Axioms

In this course, we will be considering many sets specified as the closure of some base set under some family of relations. We'll start with the (natural) numbers, for which Giuseppe Peano (1858–1932) proposed basic axioms equivalent to the following:

The Axiom of Numbers

$\mathbb{N}$ is a set, 0 is an element of $\mathbb{N}$, and suc is a function $\mathbb{N} \to \mathbb{N}$, such that:

Inductive Property $\mathbb{N}$ is the closure of $\{0\}$ under suc.

Injective Property (a) suc is injective.

(b) 0 is not in the range of suc.

The Inductive Property means that any set of numbers that contains 0 and is closed under suc includes every number. In other words: we can prove that every number has a certain property by proving (i) that 0 has the property and (ii) that for any number *n*, if *n* has the property, then suc *n* has the property.

Example

Theorem

No number is its own successor.

Proof: By induction. Base case: $0 \neq \operatorname{suc} 0$, since 0 is not in the range of suc.

Inductive step: suppose n is a number such that $n \neq \operatorname{suc} n$. Then since suc is injective, $\operatorname{suc} n \neq \operatorname{suc}(\operatorname{suc} n)$.

- Here the property we are interested in is *not being your own successor*. At the induction step, we are showing that for any n, if n has the property, then $\operatorname{suc} n$ has the property.

The role of the Injective Property

Intuitively, the Injective Property means that every natural number can be *specified in exactly one way* by starting with 0 and applying suc (‘no confusion’).

The key use of this is in establishing the following (which we’ll prove later):

Recursion Theorem for Numbers

Suppose B is a set; $z \in B$; and $s : B \to B$. Then there is a *unique* function $f : \mathbb{N} \to B$ such that $f0 = z$ and for all $n \in \mathbb{N}$, $f(\mathrm{suc}\, n) = s(fn)$.

This gives us an *exceedingly* useful way of defining functions whose domain is $\mathbb{N}$.

The Recursion Theorem at work

For example, the following counts as a definition:

Definition

Let double be the function $\mathbb{N} \to \mathbb{N}$ such that $\operatorname{double} 0 = 0$ and for any n, $\operatorname{double}(\operatorname{suc} n) = \operatorname{suc}(\operatorname{suc}(\operatorname{double} n))$.

The Recursion Theorem tells us that there is a unique function that meets these two conditions, so the definition is legitimate.

We can use our definition to calculate the value of the function on any given number:

$$\begin{aligned} \operatorname{double} 2 &= \operatorname{suc}(\operatorname{suc}(\operatorname{double} 1)) \\ &= \operatorname{suc}(\operatorname{suc}(\operatorname{suc}(\operatorname{suc}(\operatorname{double} 0)))) \\ &= \operatorname{suc}(\operatorname{suc}(\operatorname{suc}(\operatorname{suc} 0))) = 4 \end{aligned}$$

Here, we define $1 := \operatorname{suc} 0$, $2 := \operatorname{suc} 1$, $3 := \operatorname{suc} 2$, $4 := \operatorname{suc} 3$, etc.

Addition

Definition

For any $k \in \mathbb{N}$, $\operatorname{add} k$ is the unique function $f : \mathbb{N} \to \mathbb{N}$ such that $f0 = k$ and $f(\operatorname{suc} n) = \operatorname{suc}(fn)$ for all $n \in \mathbb{N}$.

The Recursion Theorem tells us that for any given k there is a unique function that meets these conditions.

We define $n + m$ as short for $(\operatorname{add} n)m$. So the conditions can be rewritten as:

$$n + 0 = n$$
$$n + \operatorname{suc} m = \operatorname{suc}(n + m)$$

N.B.: we haven't yet proved that $n + m = m + n$. So it does not go without saying that $0 + n = n$ or that $\operatorname{suc} n + m = \operatorname{suc}(n + m)$: in fact we'll need to prove these things.

Multiplication

Definition

For any $k \in \mathbb{N}$, $\mathrm{multiply}\,k$ is the unique function $f : \mathbb{N} \to \mathbb{N}$ such that $f0 = 0$ and $f(\mathrm{suc}\,n) = (\mathrm{add}\,k)(fn)$ for all $n \in \mathbb{N}$.

We define $n \times m$ or nm as short for $(\mathrm{multiply}\,n)m$. So the conditions can be rewritten as:

$$\begin{aligned} n \times 0 &= 0 \\ n \times \mathrm{suc}\,m &= m + (n \times m) \end{aligned}$$

N.B.: we haven't yet proved that $n \times m = m \times n$. So it does not go without saying that $0 \times n = 0$ or that $(\mathrm{suc}\,n) \times m = n + (n \times m)$: in fact we'll need to prove these things.