Chapter 5

Inductive definitions

This chapter shows where induction principles come from. It is an introduction to the theory of inductively-defined sets. It provides general methods for defining sets recursively, and general induction rules to accompany inductively-defined sets.

5.1 Sets defined by rules—examples

Often a set is described in the following way. Some clauses stipulate that certain basic elements are to be in the set; then clauses are given stipulating further elements of the set in terms of elements already included. Implicitly, only elements produced in these stipulated ways are to be included in the set. This gives a kind of recipe for making a set: first put in the basic elements; then, conditional on certain elements being in, add others. Sets described in this way are called *inductively defined.*

Inductively defined sets are ubiquitous, but not always presented in the same way. To stress the commonality in their form of definition we'll present inductively-defined sets via rules. A rule instance comprises its premises and a conclusion

$$\frac{x_1, x_2, \cdots}{y} .$$

The intended interpretation is: if the premises $x_1, x_2, \cdots$ are in the set being defined, then so is the conclusion y. The premises may form an empty set, in which case the rule simply expresses that the conclusion y is in the set. The following examples only give a limited idea of the range of applications of inductive definitions—you'll meet them again and again, in applications as diverse as semantics, logic, verification, logic programming, datatypes, compiler construction, security, probability, ...

Example: The set of nonnegative integers $\mathbb{N}_0$ can be thought of as being generated in the following way: zero, 0, is a nonnegative integer; if n is a nonnegative integer, then so is $n+1$. We can format these clauses in the form of rules:

$$\frac{}{0} \qquad \frac{n}{n+1} \quad \text{, where } n \in \mathbb{N}_0.$$

We can alternatively consider $\mathbb{N}_0$ as generated by the rules:

$$\frac{}{0} \qquad \frac{0, 1, \cdots, (n-1)}{n} \quad \text{, where } n \in \mathbb{N}_0.$$

□

Example: The set of strings Σ^* over an alphabet of symbols Σ are defined by these clauses: ε is a string, the empty string; if x is a string and $a \in \Sigma$, then the concatenation ax is a string. Formatted as rules:

$$\frac{}{\varepsilon} \qquad \frac{x}{ax}\ a \in \Sigma$$

where we insist in the side condition that only symbols from the alphabet are used in making strings. (The set of *lists* over elements in Σ would be constructed in the same way, though generally writing [] for the empty list, and $a :: x$ for the concatenation of a in Σ to the front of a list x.)

The rules for producing nonnegative integers exampled above assumed the prior existence of such integers. At the dawn of thought, 'caveman numbers' could have been invented as strings of scratches '$|$' generated by the rules

$$\frac{}{|} \qquad \frac{x}{x|}$$

where x stands for a string of scratches. Repeated use of the rules would lead to

$$| \qquad || \qquad ||| \qquad |||| \qquad ||||| \qquad \cdots .$$

This shows how the natural numbers can be built from scratch! □

Example: The syntax of Boolean propositions can be described by

$$\mathtt{A}, \mathtt{B}, ... ::= \mathtt{a}, \mathtt{b}, \mathtt{c}, \cdots \mid \mathtt{T} \mid \mathtt{F} \mid \mathtt{A} \wedge \mathtt{B} \mid \mathtt{A} \vee \mathtt{B} \mid \neg \mathtt{A}$$

where $\mathtt{a}, \mathtt{b}, \mathtt{c} \cdots \in \mathtt{Var}$ belong to a set of propositional variables, $\mathtt{Var}$. We might instead describe the syntax of propositions by rules of the form:

$$\frac{}{\mathtt{a}}\ \mathtt{a} \in \mathtt{Var} \qquad \frac{}{\mathtt{T}} \qquad \frac{}{\mathtt{F}}$$

$$\frac{\mathtt{A} \quad \mathtt{B}}{\mathtt{A} \wedge \mathtt{B}} \qquad \frac{\mathtt{A} \quad \mathtt{B}}{\mathtt{A} \vee \mathtt{B}} \qquad \frac{\mathtt{A}}{\neg \mathtt{A}}$$

Each rule gives a step in the way of building up a Boolean proposition. Some rules say how to build propositions like $\mathtt{A} \wedge \mathtt{B}$ out of propositions $\mathtt{A}$ and $\mathtt{B}$ built earlier. Others assert that there are basic propositions like $\mathtt{T}$, or $\mathtt{a}$ where $\mathtt{a} \in \mathtt{Var}$. □

Exercise 5.1 Write down rules to define the set of binary trees with leaves in an alphabet Σ. □

5.2 Inductively-defined sets

We are interested in the general problem of defining a set by rules of the kind we have seen in the examples.

In essence, an instance of a rule has the form of a pair (X/y) consisting of a set X, the *premises*, and a *conclusion* y. In general X might be empty or even infinite. When there is rule of the form $(\emptyset/y)$ we will call y an *axiom*. We say a rule (X/y) is *finitary* when the set X is finite; then the rule will be of the form $(\{x_1, \ldots, x_n\}/y)$, possibly with empty premises.

All examples of the previous section are associated with their own *set* of rule instances. For example, for strings Σ^* the rule instances form the set

$$\{(\emptyset/\varepsilon)\} \cup \{(\{x\}/ax) \mid x \in \Sigma^* \ \&\ a \in \Sigma\} \ ,$$

consisting of all instantiations of the rules used in building up strings. We gave two forms of rules for generating the nonnegative integers $\mathbb{N}_0$. For the first the set of rule instances is

$$\{(\emptyset/0)\} \cup \{(\{n\}/n+1) \mid n \in \mathbb{N}_0\} \ ,$$

while for the second the set is

$$\{(\{0, \cdots, (n-1)\}/n) \mid n \in \mathbb{N}_0\} \ .$$

A set of rule instances R specifies a way to build a set. A particular rule instance (X/y) is intended to say that if all the elements of X are in the set then so is y. We look for the least set with this property. If it exists this should be the set inductively defined by the rules.

Suppose we are given a set of rule instances R. We say a set Q is *closed* under the rule instances R, or simply *R-closed*, iff for all rule instances (X/y)

$$X \subseteq Q \Rightarrow y \in Q \ .$$

In other words, a set is closed under the rule instances if whenever the premises of any rule instance lie in the set so does its conclusion. In particular, an R-closed set must contain all the axioms.

Assume a set of rule instances R. Consider the collection of all R-closed sets:

$$\{Q \mid Q \text{ is } R\text{-closed}\}\ .$$

This collection is nonempty as, for example, the set

$$\{y \mid \exists X.\ (X/y) \in R\}$$

is clearly R-closed. Thus we can form its intersection

$$I_R = \bigcap\{Q \mid Q \text{ is } R\text{-closed}\}\ .$$

The important fact is that I_R is itself R-closed. To see this argue as follows: Let $(X/y) \in R$. Suppose $X \subseteq I_R$. Let Q be any R-closed subset. Then $X \subseteq Q$ and consequently $y \in Q$, as Q is R-closed. Hence $y \in I_R$.

Summarising what we have just shown:

Proposition 5.2 *With respect to a set of rule instances R,*
(i) *I_R is R-closed, and*
(ii) *if Q is an R-closed set then $I_R \subseteq Q$.*

The set I_R is often described as the set *inductively defined* by R. Proposition 5.2 will supply us with a very useful proof principle for showing a property holds of all the elements of I_R. The earlier examples give an idea of how widespread inductively-defined sets are.

5.3 Rule induction

Suppose we wish to show a property $P(x)$ is true of all elements $x \in I_R$, the set inductively-defined by a set of rule instances R. The conditions (i) and (ii) in Proposition 5.2 above furnish a method. Define the set

$$Q = \{x \in I_R \mid P(x)\}\ .$$

The property $P(x)$ is true of all $x \in I_R$ iff $I_R \subseteq Q$. By condition (ii), to show $I_R \subseteq Q$ it suffices to show that Q is R-closed. This requires that for all rule instances (X/y) that

$$(\forall x \in X.\ x \in I_R \ \&\ P(x)) \Rightarrow (y \in I_R \ \&\ P(y))\ .$$

But I_R is R-closed by (i), so this will follow precisely when

$$(\forall x \in X.\ x \in I_R \ \&\ P(x)) \Rightarrow P(y)\ .$$

We have obtained an important, general proof principle.

The principle of rule induction
Let I_R be inductively-defined by R. Then $\forall x \in I_R.\ P(x)$ if for all rule instances (X/y) in R,

$$(\forall x \in X.\ x \in I_R \ \&\ P(x)) \Rightarrow P(y)\ .$$

(The property $P(x)$ is called the *induction hypothesis*.)

[In other words to prove $\forall x \in I_R.\ P(x)$ it suffices to show that $\forall x \in X.\ P(x)$ implies $P(y)$ only for all rule instances (X/y) *with* $X \subseteq I_R$.]

Notice for rule instances of the form (X/y), with $X = \emptyset$, the condition in the statement of rule induction is equivalent to $P(y)$. Certainly then $\forall x \in X.\ x \in I_R \ \&\ P(x)$ is vacuously true because any x in $\emptyset$ satisfies $P(x)$—there are none.

Supposing the rule instances R are finitary, the statement of rule induction amounts to the following. For rule instances R, we have $\forall y \in I_R.\ P(y)$ iff for all axioms

$$\frac{}{y}$$

$P(y)$ is true, and for all rule instances

$$\frac{x_1, \ldots, x_n}{y}$$

if $x_k \in I_R$ & $P(x_k)$ is true for all the premises, when k ranges from 1 to n, then $P(y)$ is true of the conclusion.

The principle of rule induction is very useful to show a property is true of all the elements in an inductively-defined set. It has many well-known instances.

Examples: Refer to the examples of rules beginning this chapter.

Nonnegative integers $\mathbb{N}_0$: The rules $(\emptyset/0)$ and $(\{n\}/(n+1))$, for a number n, yield *mathematical induction* as a special case of rule induction.

The alternative rules $(\emptyset/0)$ and $(\{0, 1, \cdots, (n-1)\}/n)$, for a number n, yield *course-of-values induction*, the principle that says: A property $P(n)$ holds for all nonnegative numbers n iff for all $n \in \mathbb{N}_0$

$$(\forall m < n.\ P(m)) \Rightarrow P(n)\ .$$

Notice what happens when $n = 0$. Then there are no $m \in \mathbb{N}_0$ with $m < 0$, so the condition of the implication is vacuously true and the implication amounts to $P(0)$. Course-of-values induction is useful when truth of a property at n can depend on its truth at earlier values other than just its immediate predecessor.

Strings Σ^*: With the rules for strings over an alphabet Σ rule induction specialises to this principle: a property $P(x)$ holds of all strings $x \in \Sigma^*$ iff

$$\begin{array}{l} P(\varepsilon) \text{ and} \\ \forall a \in \Sigma,\ x \in \Sigma^*.\ P(x) \Rightarrow P(ax)\ . \end{array}$$

(Essentially the same induction principle works for lists.)

Boolean propositions: With the rules for the syntax of Boolean propositions, rule induction specialises to *structural induction.*

Exercise 5.3 Justify the following "special principle of rule induction." Let I_R be defined by a set of rule instances R. Let $A \subseteq I_R$. Then $\forall a \in A.\ Q(a)$ if for all rule instances (X/y) in R, with $X \subseteq I_R$ and $y \in A$,

$$(\forall x \in X \cap A.\ Q(x)) \Rightarrow Q(y).$$

[Hint: Take property $P(x)$ to be

$$P(x) \text{ iff } (x \in A \Rightarrow Q(x))$$

in the statement of rule induction.] □

Exercise 5.4 Based on your rules for binary trees with leaves in Σ (*cf.* Exercise 5.1), write down the corresponding principle of rule induction. □

Exercise 5.5 The set of well-bracketed strings is the subset of strings over symbols [and] defined inductively as follows:

[ ] is well-bracketed;

if x is well-bracketed, then $[x]$ is well-bracketed;

if x and y are well-bracketed, then xy is well-bracketed.

State the principle of rule induction for well-bracketed strings. Show the number of left brackets [equals the number of right brackets] in any well-bracketed string. □

Exercise 5.6 A simple language is defined with symbols a and b. The grammar of this language has the rules:

- ab is a word;
- if ax is a word, then axx is a word (where x is any string of symbols);
- if $abbbx$ is a word, then ax is a word.

(i) Is $abbbbb$ a word? Either exhibit a derivation, or prove there isn't one.

(ii) Is $abbb$ a word? Either exhibit a derivation, or prove there isn't one.

(iii) Characterise the strings which are words. Prove your characterisation is correct. □

Exercise 5.7 The set S is defined to be the least subset of natural numbers $\mathbb{N}$ such that:

$1 \in S$;

if $n \in S$, then $3n \in S$;

if $n \in S$ and $n > 2$, then $(n - 2) \in S$.

Show that $S = \{m \in \mathbb{N} \mid \exists r, s \in \mathbb{N} \cup \{0\}. \quad m = 3^r - 2s\}$. Deduce that S is the set of odd numbers. □

Exercise 5.8 Let I be a nonempty subset of the natural numbers $\mathbb{N} = \{1, 2, 3, \cdots\}$.
The set S is defined to be least subset of $\mathbb{N}$ such that

$I \subseteq S$, and
if $m, n \in S$ and $m < n$, then $(n - m) \in S$.

Define h to be the least member of S. This question guides you through to a proof that h coincides with the *highest common factor* of I, written $hcf(I)$, and defined to be the natural number with the properties that

$hcf(I)$ divides n for every element $n \in I$, and
if k is a natural number which divides n for every $n \in I$, then k divides $hcf(I)$.

(a) The set S may also be described as the least subset of $\mathbb{N}$ closed under certain rules. Describe the rules. Write down a principle of rule induction appropriate for the set S.

(b) Show by rule induction that $hcf(I)$ divides n for every $n \in S$.

(c) Let $n \in S$. Establish that

$$\text{if } \ p \cdot h < n \ \text{ then } \ (n - p \cdot h) \in S$$

for all nonnegative integers p.

(d) Show that h divides n for every $n \in S$. [Hint: suppose otherwise and derive a contradiction.]

(e) Why do the results of (b) and (d) imply that $h = hcf(I)$?

□

5.3.1 Transitive closure of a relation

Suppose that R is a relation on a set U. Its *transitive closure*, written R^+, is defined to be the least relation T such that T includes R and T is transitive, *i.e.*

$$R \subseteq T \text{ and}$$
$$(a, b) \in T \ \& \ (b, c) \in T \Rightarrow (a, c) \in T \ .$$

An element of R^+, *i.e.* a pair $(a, b) \in R^+$, is either in the original relation R or put in through enforcing transitivity. This is captured by the following rules for pairs in $U \times U$:

$$\frac{}{(a, b)} \ (a, b) \in R \qquad\qquad \frac{(a, b) \quad (b, c)}{(a, c)} \ . \tag{1}$$

In other words the transitive closure R^+ is inductively defined by these rules.

You may have seen another way to characterise the transitive closure of R. Define an R-chain from a to b to consist of pairs $(a_1, a_2), (a_2, a_3), \cdots, (a_{n-1}, a_n)$ in R with $a = a_1$ and $b = a_n$. Then, $(a, b) \in R^+$ iff there is an R-chain from a to b.
To see this, let

$$S = \{(a, b) \mid \text{ there is an } R\text{-chain from } a \text{ to } b\} \ .$$

First observe that

$$R \subseteq S \text{ and } (a, b) \in S \ \& \ (b, c) \in S \Rightarrow (a, c) \in S \ ,$$

the former because pairs in R form 1-link R-chains, the latter because we can concatenate two R-chains to get an R-chain. It follows that

$$R^+ \subseteq S \ .$$

To show equality, we need the converse too. This follows by mathematical induction on $n \in \mathbb{N}$ with induction hypothesis:

$$\text{for all } R\text{-chains } (a_1, a_2), (a_2, a_3), \cdots, (a_{n-1}, a_n) \text{ we have } (a_1, a_n) \in R^+ \ .$$

The basis of the induction, when $n = 1$, follows directly as $R \subseteq R^+$. The induction step uses, in addition, the transitivity of R^+.

Exercise 5.9 Show the transitive closure of a relation R is the least relation T such that:

$$R \subseteq T \text{ and } (a, b) \in R \ \& \ (b, c) \in T \Rightarrow (a, c) \in T \ .$$

□

One way to define the *reflexive, transitive closure* R^* of a relation R on a set U is as

$$R^* = \mathsf{id}_U \cup R^+ \ .$$

Exercise 5.10 Let R be a relation on a set U. Show that R^* is the least relation that includes R and is reflexive and transitive. □

Exercise 5.11 Let R be a relation on a set U. Define $R^0 = \mathsf{id}_U$, the identity relation on the set U, and $R^1 = R$ and inductively, assuming R^n is defined, define

$$R^{n+1} = R \circ R^n \ .$$

So, R^n is the relation $R \circ \cdots \circ R$, obtained by taking n compositions of R. Show the transitive closure of R is the relation

$$R^+ = \bigcup_{n \in \mathbb{N}_0} R^{n+1} \ ,$$

and that the transitive, reflexive closure of a relation R on X is the relation

$$R^* = \bigcup_{n \in \mathbb{N}_0} R^n \ .$$

□

Exercise 5.12 Show $(R \cup R^{-1})^*$ is an equivalence relation. Show that it is the least equivalence relation including R. Show $R^* \cup (R^{-1})^*$ need not be an equivalence relation. □

Exercise 5.13 Show that the least equivalence relation containing two equivalence relations R and S on the same set is $(R \cup S)^+$. □

5.4 Derivation trees

Another important way to understand inductively-defined sets as generated by rules is via the notion of a *derivation tree*, or *derivation*. An inductively-defined set consists of precisely those elements for which there is a derivation. In this section we'll assume a set of rule instances R which are all finitary, though the ideas generalise straightforwardly to infinitary rules.

We are familiar with informal examples of derivations from games, like chess, draughts or bridge, where it's usual to discuss a particular play of a game leading up to a winning position. In the idealised view of mathematics, as a formal game of deriving theorems from rules, a proof is a derivation of a theorem from the rules of mathematics. As the example of proofs in mathematics makes clear, derivations can have much more informative structure than the, often simpler, things they are intended to derive; finding proofs in mathematics is highly nontrivial because the form an assertion takes rarely determines the structure of its possible proofs.

As a simple example here's a derivation for the Boolean proposition $\neg\mathtt{a}\wedge(\mathtt{b}\vee\mathtt{T})$ using the rules of syntax for forming Boolean propositions:

$$\dfrac{\dfrac{\dfrac{}{\mathtt{a}}}{\neg\mathtt{a}} \qquad \dfrac{\dfrac{}{\mathtt{b}} \qquad \dfrac{}{\mathtt{T}}}{\mathtt{b}\vee\mathtt{T}}}{\neg\mathtt{a}\wedge(\mathtt{b}\vee\mathtt{T})}$$

It has the form of a tree with the conclusion at the root and with axioms at the leaves. It is built by stacking rules together, matching conclusions with premises.

The idea is that rules lift to rules generating derivations; we build a new derivation by stacking derivations on top of matching premises of a rule. A derivation of an element y takes the form of a tree which is either an instance of an axiom

$$\dfrac{}{y}$$

or of the form

$$\dfrac{\dfrac{\vdots}{x_1},\ldots,\dfrac{\vdots}{x_n}}{y}$$

which includes derivations of $x_1,\ldots,x_n$, the premises of a rule with conclusion y. In such a derivation we think of $\dfrac{\vdots}{x_1},\cdots,\dfrac{\vdots}{x_n}$ as subderivations of the larger derivation of y.

In set notation, an *R-derivation* of y is either a rule

$$(\emptyset/y)$$

or a pair

$$(\{d_1,\cdots,d_n\}/y)$$

where $(\{x_1,\cdots,x_n\}/y)$ is a rule and d_1 is an R-derivation of x_1, …, and d_n is an R-derivation of x_n.

As the formulation makes clear, the set of all R-derivations is inductively-defined. In this case rule induction specialises to another useful proof principle.

Induction on derivations
Let $P(d)$ be a property of R-derivations d. Then, $P(d)$ holds for all R-derivations d iff for all rule instances $(\{x_1,\cdots,x_n\}/y)$ in R and R-derivations d_1 of x_1, …, and d_n of x_n,

$$P(d_1)\ \&\ \cdots\ \&\ P(d_n)\Rightarrow P(\{d_1,\cdots,d_n\}/y)\ .$$

(As usual, the property $P(d)$ is called the induction hypothesis.)

In practice it is easier to apply induction on derivations than its rather formal statement might suggest. A proof by induction on derivations splits into cases according to the last rule in the derivation. In each case, it is required to show that a derivation

$$\frac{\dfrac{\vdots}{x_1}, \ldots, \dfrac{\vdots}{x_n}}{y}$$

inherits a desired property from its subderivations $\dfrac{\vdots}{x_1}, \cdots, \dfrac{\vdots}{x_n}$. Induction on derivations is illustrated in the proof of the following fundamental result.

Theorem 5.14 *An element $y \in I_R$ iff there is an R-derivation of y.*

Proof.
‘only if’: Consider the set

$$D = \{y \mid \text{ there is an } R\text{-derivation of } y\} \ .$$

The set D is R-closed as given any rule (X/y) and derivations for all its premises X we can construct a derivation of y. Thus $I_R \subseteq D$.
’if’: A simple induction on derivations shows that $y \in I_R$ for any derivation of y. The argument: Take as induction hypothesis the property that holds of a derivation of y precisely when $y \in I_R$. Consider any rule $(\{x_1, \cdots, x_n\}/y)$ and derivations d_1 of x_1, …, and d_n of x_n for which $x_1 \in I_R$, …, and $x_n \in I_R$. Then, as I_R is R-closed, $y \in I_R$. □

It can sometimes be easier to attach a property to a derivation, which encodes the whole history of how an element came to be in an inductively-defined set, than to an element standing alone. If the rules are such that the conclusions determine the rules uniquely there is no advantage (or disadvantage) in using induction on derivations over straight rule induction.