induction

Canonical name	Induction
Date of creation	2013-03-22 12:24:27
Last modified on	2013-03-22 12:24:27
Owner	Daume (40)
Last modified by	Daume (40)
Numerical id	14
Author	Daume (40)
Entry type	Topic
Classification	msc 03B48
Classification	msc 03F07
Related topic	TransfiniteInduction
Related topic	PrincipleOfFiniteInduction
Defines	inductive order
Defines	partial well-order

Induction is the name given to a certain kind of proof, and also to a (related) way of defining a function. For a proof, the statement to be proved has a suitably *ordered* set of cases. Some cases (usually one, but possibly zero or more than one), are proved separately, and the other cases are deduced from those. The deduction goes by contradiction, as we shall see. For a function, its *domain* is suitably ordered. The function is first defined on some (usually nonempty) subset of its domain, and is then defined at other points x in terms of its values at points y such that $y < x$.

1 Elementary proof by induction

Proof by induction is a variety of proof by contradiction, relying, in the elementary cases, on the fact that every non-empty set of natural numbers has a least element. Suppose we want to prove a statement $F(n)$ which involves a natural number n. It is enough to prove:

1) If $n \in \mathbb{N}$, and $F(m)$ is true for *all* $m \in \mathbb{N}$ such that $m < n$, then $F(n)$ is true.

or, what is the same thing,

2) If $F(n)$ is false, then $F(m)$ is false for *some* $m < n$.

To see why, assume that $F(n)$ is false for some n. Then there is a *smallest* $k \in \mathbb{N}$ such that $F(k)$ is false. Then, by hypothesis, $F(n)$ is true for all $n < k$. By (1), $F(k)$ is true, which is a contradiction.

(If we don't regard induction as a kind of proof by contradiction, then we have to think of it as supplying some kind of sequence of proofs, of unlimited length. That's not very satisfactory, particularly for transfinite inductions, which we will get to below.)

Usually the initial case of $n = 0$, and sometimes a few cases, need to be proved separately, as in the following example. Write $B_n = \sum_{k=0}^{n} k^2$. We claim

$$B_n = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} \text{ for all } n \in \mathbb{N}$$

Let us try to apply (1). We have the inductive hypothesis (as it is called)

$$B_m = \frac{m^3}{3} + \frac{m^2}{2} + \frac{m}{6} \text{ for all } m < n$$

which tells us something *if* $n > 0$. In particular, setting $m = n - 1$,

$$B_{n-1} = \frac{(n-1)^3}{3} + \frac{(n-1)^2}{2} + \frac{n-1}{6}$$

Now we just add n^2 to each side, and verify that the right side becomes $\frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}$. This proves (1) for nonzero n. But if $n = 0$, the inductive hypothesis is vacuously true, but of no use. So we need to prove $F(0)$ separately, which in this case is trivial.

Textbooks sometimes distinguish between *weak* and *strong* (or *complete*) inductive proofs. A proof that relies on the inductive hypothesis (1) is said to go by strong induction. But in the sum-of-squares formula above, we needed only the hypothesis $F(n-1)$, not $F(m)$ for all $m < n$. For another example, a proof about the Fibonacci sequence might use just $F(n-2)$ and $F(n-1)$. An argument using only $F(n-1)$ is referred to as weak induction.

2 Definition of a function by induction

Let's begin with an example, the function $\mathbb{N} \to \mathbb{N}$, $n \mapsto a^n$, where a is some integer > 0. The inductive definition reads

$$
\begin{aligned}
a^0 &= 1 \\
a^n &= a(a^{n-1}) \text{ for all } n > 0
\end{aligned}
$$

Formally, such a definition requires some justification, which runs roughly as follows. Let T be the set of $m \in \mathbb{N}$ for which the following definition "has no problem".

$$
\begin{aligned}
a^0 &= 1 \\
a^n &= a(a^{n-1}) \text{ for } 0 < n \le m
\end{aligned}
$$

We now have a finite sequence f_m on the interval $[0, m]$, for each $m \in T$. We verify that any f_l and f_m have the same values throughout the intersection of their two domains. Thus we can define a single function on the *union* of the various domains. Now suppose $T \ne \mathbb{N}$, and let k be the least element of $\mathbb{N} - T$. That means that the definition has a problem when $m = k$ but not when $m < k$. We soon get a contradiction, so we deduce $T = \mathbb{N}$. That means that the union of those domains is all of $\mathbb{N}$, i.e. the function a^n is defined, unambiguously, throughout $\mathbb{N}$.

Another inductively defined function is the Fibonacci sequence, q.v.

We have been speaking of the inductive definition of a *function*, rather than just a sequence (a function on $\mathbb{N}$), because the notions extend with little change to transfinite inductions. An illustration *par excellence* of inductive

proofs and definitions is Conway's theory of surreal numbers. The numbers and their algebraic laws of composition are defined entirely by inductions which have no special starting cases.

3   Minor variations of the method

The reader can figure out what is meant by "induction starting at k", where k is not necessarily zero. Likewise, the term "downward induction" is self-explanatory.

A common variation of the method is proof by induction on a *function* of the index n. Rather than spell it out formally, let me just give an example. Let n be a positive integer having no prime factors of the form $4m + 3$. Then $n = a^2 + b^2$ for some integers a and b. The usual textbook proof uses induction on a function of n, namely the number of prime factors of n. The induction starts at 1 (i.e. either $n = 2$ or prime $n = 4m + 1$), which in this instance is the only part of the proof that is not quite easy.

4   Well-ordered sets

An ordered set $(S, \leq)$ is said to be well-ordered if any nonempty subset of S has a least element. The criterion (1), and its proof, hold without change for any well-ordered set S in place of $\mathbb{N}$ (which is a well-ordered set). But notice that it won't be enough to prove that $F(n)$ implies $F(n + 1)$ (where $n + 1$ denotes the least element $> n$, if it exists). The reason is, given an element m, there may exist elements $< m$ but no element k such that $m = k + 1$. Then the induction from n to $n + 1$ will fail to "reach" m. For more on this topic, look for "limit ordinals".

Informally, any variety of induction which works for ordered sets S in which a segment $S_x = \{y \in S | y < x\}$ may be infinite, is called "transfinite induction".

5   Noetherian induction

An ordered set S, or its order, is called Noetherian if any non-empty subset of S has a maximal element. Several equivalent definitions are possible, such as

the "ascending chain condition": any strictly increasing sequence of elements of S is finite. The following result is easily proved by contradiction.

Principle of Noetherian induction: Let $(S, \leq)$ be a set with a Noetherian order, and let T be a subset of S having this property: if $x \in S$ is such that the condition $y > x$ implies $y \in T$, then $x \in T$. Then $T = S$.

So, to prove something "$F(x)$" about every element x of a Noetherian set, it is enough to prove that "$F(z)$ for all $z > y$" implies "$F(y)$". This time the induction is going downward, but of course that is only a matter of notation. The opposite of a Noetherian order, i.e. an order in which any strictly decreasing sequence is finite, is also in use; it is called a partial well-order, or an ordered set having no infinite antichain.

The standard example of a Noetherian ordered set is the set of ideals in a Noetherian ring. But the notion has various other uses, in topology as well as algebra. For a nontrivial example of a proof by Noetherian induction, look up the Hilbert basis theorem.

6 Inductive ordered sets

An ordered set $(S, \leq)$ is said to be inductive if any totally ordered subset of S has an upper bound in S. Since the empty set is totally ordered, any inductive ordered set is non-empty. We have this important result:

Zorn's lemma: Any inductive ordered set has a maximal element.

Zorn's lemma is widely used in existence proofs, rather than in proofs of a property $F(x)$ of an arbitrary element x of an ordered set. Let me sketch one typical application. We claim that every vector space has a basis. First, we prove that if a free subset F, of a vector space V, is a maximal free subset (with respect to the order relation $\subset$), then it is a basis. Next, to see that the set of free subsets is inductive, it is enough to verify that the union of any totally ordered set of free subsets is free, because that union is an upper bound on the totally ordered set. Last, we apply Zorn's lemma to conclude that V has a maximal free subset.