

Strong Induction*

Graeme Taylor

October 22, 2002

Strong Induction is a variant on Proof by Induction whereby any cases $P(m)$, $m \leq k$, instead of just $P(k)$, are used to prove the statement $P(k + 1)$ and hence the general statement $P(n)$.

What does this mean in practice? Well, typically mathematical induction comprises of the following steps:

- Set up a statement $P(n)$, $n \in \mathbb{N}$. (or some well ordered integers, such as $n \in \mathbb{Z}$, $n \geq 0$)
- Confirm for the first value- usually 1.
- Assume $P(k)$ is true, and use it to show that $P(k + 1)$ is true- that is, one case implies the next. Hence, $P(n)$ is true for all n greater than or equal to the value chosen in the second step. If that number was 1, $P(n)$ is true for all natural numbers.

Why then is strong induction necessary? Although the above steps are sufficient for a proof, it might not actually be possible to carry out the final stage- that is, show $P(k)$ implies $P(k + 1)$. An example is finding prime factors of a number. Our statement $P(n)$ would be "*n is the product of primes if $n \in \mathbb{N}$ and $n > 1$* ". (This includes the possibility that n is prime in which case it is a 'product' of just one prime, itself) Checking with $P(2)$ works- the statement claims 2 is a product of primes which is true. With ordinary induction we would then assume $P(k)$, that is "*k is the product of primes...*" and try to use it to show $P(k + 1)$.

Unfortunately, knowing that k can be factorised into primes doesn't tell us how or even if $k + 1$ might be factorised- for instance, knowing that 14 is 2×7 is of no use when trying to find the prime factors of 15. Thus ordinary induction fails not because it isn't true but because we can't show it. Strong Induction solves this problem by allowing us to prove another statement, $P'(n)$, of the form "*P(n) is true for all $m \leq n$, $m \in \mathbb{N}$* ". Proving $P'(n)$ proves $P(n)$ for all n as desired, and $P'(n)$ is easier to prove as it allows us to use any previous $P(m)$ rather than just $P(k)$ to show that $P(k)$ implies $P(k + 1)$.

*First appeared on Everything2, at http://www.everything2.com/index.pl?node_id=1377092

Going back to our example of prime decomposition, our modified $P(n)$ is the statement "*Any natural number $m \leq n$ is a product of primes (or $m = 1$).*" Then $P(2)$ now states that 1 and 2 are either the product of primes or equal to 1- which is true, so we'll assume $P(k)$.

$P(k + 1)$ is then the statement "*Any natural number $m \leq (k + 1)$ is a product of primes (or $m = 1$).*" Well, having assumed $P(k)$ we already believe all values of $m \leq k$ to be products of primes (or $m = 1$), so all we need to show is that $m = (k + 1)$ is a product of primes. If $k + 1$ is prime then there is nothing to be done. Supposing it is not prime but is instead the product of two values $a, b \in \mathbb{N}$, then both a and b are less than or equal to k - and so having assumed $P(k)$, they can be expressed as the product of primes. So $k + 1 = ab$ can also be expressed as the product of primes. So given $P(k)$, we have $P(k + 1)$. Given $P(2)$, $P(n)$ is therefore true for all $n \in \mathbb{N}$, $n \geq 2$.

Generally, strong induction is of use when carrying out functions such as multiplication or division, which relate to much earlier cases of $P(m)$ that an ordinary induction proof would not have access to. Or as my numbers lecturer puts it, "*this is induction for elephants, because elephants never forget. We've done induction for hamsters, but one elephant can replace a whole load of hamsters....*"