Proof by strong induction

Here is the theorem we proved in class using strong induction.

Theorem A. *Let n be a natural number. Then n has a* ***binary representation****: we can write*

$$n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_s},$$

where the exponents $m_1, \ldots, m_s$ are distinct non-negative integers (no repeats).

Proof. The proof is by strong induction on n.

Base case: For the base case, let $n = 1$. The binary representation of 1 is

$$1 = 2^0.$$

Notice that there are no repeated exponents (because there is only a single power of 2 here). Thus, the theorem holds for $n = 1$.

Induction step: Now, let n be any natural number. We assume, for our *strong inductive hypothesis*, that the theorem is true for every natural number k such that $1 \leq k \leq n$. That is, we assume that *all of the numbers* $1, 2, 3, \ldots, n$ have a binary representation.

We now wish to show that $n + 1$ will have a binary representation. Let $a \geq 0$ be the largest integer such that

$$n + 1 \geq 2^a.$$

(We can find a by using the well-ordering axiom.)

If, in fact, we have an equality

$$n + 1 = 2^a,$$

then we are done, because we have represented $n+1$ as a single power of 2 (and so there are no repeated exponents).

Otherwise, the inequality is strict:

$$n + 1 > 2^a.$$

In this case, let $k = (n+1) - 2^a$. Then $1 \leq k \leq n$, and so we can apply our strong inductive hypothesis to the number k. That is, we know that k has a binary representation

$$k = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_s},$$

where there are no repeated exponents.

Thus,

$$n + 1 = 2^a + k = 2^a + 2^{m_1} + 2^{m_2} + \cdots + 2^{m_s}. \qquad (\star)$$

We claim that this is a binary representation of $n + 1$. It remains to show that there are no repeated exponents.

By assumption, there are no repeats among the m_i. Thus, we must show that $a \neq m_i$ for any i. For the sake of contradiction, assume that a is equal to one of the m_i. Relabeling if necessary, we can assume $a = m_1$. Then

$$\begin{aligned} n + 1 &= 2^a + 2^a + 2^{m_2} + \cdots + 2^{m_s} \\ &= 2 \cdot 2^a + 2^{m_2} + \cdots + 2^{m_s} \\ &= 2^{a+1} + 2^{m_2} + \cdots + 2^{m_s} \end{aligned}$$

But if this is true, then

$$n + 1 - 2^{a+1} = 2^{m_2} + \cdots + 2^{m_s} \geq 0$$

implying that

$$n + 1 \geq 2^{a+1}.$$

But this contradicts the fact that a is the largest integer such that $n + 1 \geq 2^a$. We conclude that a is not equal to any of the m_i, and so the expression $(\star)$ is a binary representation of $n + 1$. That is, the theorem holds for $n + 1$.

By strong induction, the theorem is proved for every natural number. □

How did strong induction work in this proof?

In a traditional proof by induction, we show that if the theorem is true for n, then it is true for $n + 1$. That is, each "domino" knocks over the next one.

In the proof above, we proved the theorem for $n+1$ by showing it was true for **some smaller number** k, but k was not necessarily equal to n. In our "domino" analogy, each "domino" gets knocked over by a previous "domino," but it is not exactly clear which one.

For example, if $n + 1 = 53$, then in our proof we would take $2^a = 2^5 = 32$, so that $k = 53 - 32 = 21$. Then

$$53 = 2^5 + 21$$

and we inductively use the binary representation of 21 (which is $21 = 2^4 + 2^2 + 2^0$) to get a binary representation of 53. So the 53rd "domino" is knocked over by the 21st "domino."

Another example of strong induction

Recall that the **Fibonacci numbers** F_n are defined by $F_1 = F_2 = 1$ and

$$F_n = F_{n-1} + F_{n-2}$$

for $n \geq 3$.

Theorem B. *For every natural number n,*

$$F_n \geq \left(\frac{3}{2}\right)^{n-2},$$

where F_n is the nth Fibonacci number.

Proof. We proceed by strong induction on n.

Base cases: We will prove two base cases. When $n = 1$, we have

$$F_1 = 1 > \frac{2}{3} = \left(\frac{3}{2}\right)^{1-2}.$$

When $n = 2$, we have

$$F_2 = 1 = \left(\frac{3}{2}\right)^{0} = \left(\frac{3}{2}\right)^{2-2}.$$

Thus, we see that the theorem holds in these first two cases.

Inductive step: Let $n \geq 2$. We assume, for our strong inductive hypothesis, that $F_k \geq \left(\frac{3}{2}\right)^{k-2}$ is true for every natural number k such that $2 \leq k \leq n$.

Now, applying the inductive hypothesis to $k = n$ and $k = n - 1$, we obtain

$$F_{n+1} = F_n + F_{n-1} \geq \left(\frac{3}{2}\right)^{n-2} + \left(\frac{3}{2}\right)^{(n-1)-2} = \left(\frac{3}{2}\right)^{n-3}\left(\frac{3}{2} + 1\right) = \left(\frac{3}{2}\right)^{n-3}\left(\frac{5}{2}\right).$$

Since $\frac{5}{2} = \frac{10}{4} > \frac{9}{4} = \left(\frac{3}{2}\right)^2$, we conclude that

$$F_{n+1} \geq \left(\frac{3}{2}\right)^{n-3}\left(\frac{5}{2}\right) > \left(\frac{3}{2}\right)^{n-3}\left(\frac{3}{2}\right)^{2} = \left(\frac{3}{2}\right)^{(n+1)-2}.$$

By strong induction, the theorem is proved for every natural number $n \geq 2$. □

How did strong induction work in this proof?

In some sense, the proof of Theorem B feels more like a traditional induction proof than the proof of Theorem A did. The key difference, however, is in the induction step: we showed that the theorem is true for $n+1$ by using the assumption that it is true for **both** n and $n-1$. That is, we showed that any given "domino" is knocked over by *two* previous "dominoes" working together.

Because this is the nature of our inductive step—using the two previous cases to prove the next—we needed to also begin our proof with **two base cases.** Because the Fibonacci recurrence $F_n = F_{n-1} + F_{n-2}$ only begins at $n = 3$, our inductive step does not apply when $n = 1$ or $n = 2$. So we need to prove the theorem directly for these first cases (which is fortunately easy, since $F_1 = F_2 = 1$).

Once we've proved our two base cases, the inductive step takes over: The theorem is true for $n = 4$ because it is true for $n = 3$ and $n = 2$. It is true for $n = 5$ because it is true for $n = 4$ and $n = 3$. And so on.

General comments

The aim of this document is to illustrate that strong induction proofs come in two "flavors."

Strong induction argument type #1: In the inductive step, we assume the theorem is true for all k such that $1 \leq k \leq n$. In proving the theorem for $n+1$, we'll reach back and use *one* of these previous cases. Which particular previous case we'll need will depend on the theorem we are trying to prove.

Strong induction argument type #2: In the inductive step, we assume the theorem is true for all k such that $1 \leq k \leq n$. In proving the theorem for $n+1$, we'll reach back and use *multiple* previous cases. Often, these will be the cases immediately preceding $n+1$. For instance, to prove the theorem for $n+1$, we may need to use the assumption that the theorem is true for n **and** $n-1$ **and** $n-2$. How far back we need to go will depend on the theorem we are trying to prove. Because of this, we will need to begin our proof with **multiple base cases.**

Notice that the proof of Theorem A used an argument of type #1 and the proof of Theorem B used an argument of type #2.