Induction Intro

Note 3

Natural numbers start at 0, and there is always a next one. For predicates on natural numbers the *principle of induction* is: $\forall n \in \mathbb{N}, P(n) \equiv P(0) \wedge \forall n, P(n) \implies P(n+1)$.

That is, to prove $P(n)$ for natural numbers one proves $P(0)$, the *base* case, and $\forall n, P(n) \implies P(n+1)$, the *induction step*. In the induction step, the assumption that $P(n)$ is true is called the *induction hypothesis* which is typically used to argue that $P(n+1)$ is true.

An example is the statement $P(n) = \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$. The base case, $P(0)$, is the observation that $\sum_{i=0}^{0} i = 0$. In the induction step, the induction hypothesis, $P(n)$, is $\sum_{i=0}^{n} i = \frac{(n)(n+1)}{2}$. The induction step proceeds as follows:

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + n + 1 = \frac{(n)(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}.$$

The first equality follows from the definition of the notation, $\sum$, the second substitutes the induction hypothesis and the last is algebra. And what is proven is $P(n+1)$, which is that $\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$.

Another and equivalent view of the natural numbers are that there are the numbers 0 to n and then there is $n+1$. The *strong induction principle* is that

$$\forall n \in \mathbb{N}, P(n) \equiv P(0) \wedge \forall n, ((\forall k \leq n) P(k)) \implies P(n+1).$$

Here the induction hypothesis is that $P(k)$ is true for all values $k \leq n$. To prove that every natural number $n \geq 2$ can be written as a product of primes, we take the base case as $P(2)$ which can be written as 2, which is a product of a prime. And for any n, if it is prime, it can be written as itself, otherwise $n = ab$ and by the inductive hypotheses $P(a)$ and $P(b)$ is that each can be written as a product of primes. Thus, we can write n as the product of the primes in both a and b. Note here that the base case starts at 2, which illustrates that one chose the base case as is relevant to the statement being proven.

Strengthening the induction hypothesis is a technique that proves a stronger theorem. For example, the notes consider the theorem *"The sum of the first n odd numbers is a perfect square."* In fact, the notes inductively prove the stronger theorem *"The sum of the first n odd numbers is n^2."* Here, the stronger inductive hypothesis allows the induction step to proceed easily. Note that in strong induction, we assume more cases are true in the inductive hypothesis, whereas strengthening the inductive hypothesis proves a stronger claim entirely.

1 Fibonacci for Home

Note 3 Recall, the Fibonacci numbers, defined recursively as

$F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-2} + F_{n-1}$.

Prove that every third Fibonacci number is even. For example, $F_3 = 2$ is even and $F_6 = 8$ is even.

Solution:

We want to prove that for all natural numbers $k \geq 1$, F_{3k} is even.

Base case: For $k = 1$, we can see that $F_3 = 2$ is even.

Induction hypothesis: Suppose that for an arbitrary fixed value of k, F_{3k} is even.

Inductive step: We can write

$$F_{3k+3} = F_{3k+2} + F_{3k+1} = 2F_{3k+1} + F_{3k}.$$

By the induction hypothesis, we know that $F_{3k} = 2q$ for some q.

This means that we have that $F_{3k+3} = 2(F_{3k+1} + q)$, which implies that it is even. Thus, by the principles of induction we have shown that all F_{3k} are even.

2 Natural Induction on Inequality

Note 3 Prove that if $n \in \mathbb{N}$ and $x > 0$, then $(1+x)^n \geq 1 + nx$.

Solution:

- *Base Case:* When $n = 0$, the claim holds since $(1+x)^0 \geq 1 + 0x$.
- *Inductive Hypothesis:* Assume that $(1+x)^k \geq 1 + kx$ for some value of $n = k$ where $k \in \mathbb{N}$.
- *Inductive Step:* For $n = k+1$, we can show the following:

$$\begin{aligned}(1+x)^{k+1} = (1+x)^k(1+x) &\geq (1+kx)(1+x) \\ &\geq 1 + kx + x + kx^2 \\ &\geq 1 + (k+1)x + kx^2 \geq 1 + (k+1)x\end{aligned}$$

By induction, we have shown that $\forall n \in \mathbb{N}, (1+x)^n \geq 1 + nx$.

3 Make It Stronger

Note 3 Suppose that the sequence $a_1, a_2, \ldots$ is defined by $a_1 = 1$ and $a_{n+1} = 3a_n^2$ for $n \geq 1$. We want to prove that

$$a_n \leq 3^{(2^n)}$$

for every positive integer n.

(a) Suppose that we want to prove this statement using induction. Can we let our inductive hypothesis be simply $a_n \le 3^{(2^n)}$? Attempt an induction proof with this hypothesis to show why this does not work.

(b) Try to instead prove the statement $a_n \le 3^{(2^n-1)}$ using induction.

(c) Why does the hypothesis in part (b) imply the overall claim?

Solution:

(a) Let's try to prove that for every $n \ge 1$, we have $a_n \le 3^{2^n}$ by induction.

Base Case: For $n = 1$ we have $a_1 = 1 \le 3^{2^1} = 9$.
Inductive Step: For some $n \ge 1$, we assume $a_n \le 3^{2^n}$. Now, consider $n+1$. We can write:

$$a_{n+1} = 3a_n^2 \le 3(3^{2^n})^2 = 3 \times 3^{2\times 2^n} = 3 \times 3^{2^{n+1}} = 3^{2^{n+1}+1}.$$

However, what we wanted was to get an inequality of the form: $a_{n+1} \le 3^{2^{n+1}}$. There is an extra $+1$ in the exponent of what we derived.

(b) This time the induction works.

Base Case: For $n = 1$ we have $a_1 = 1 \le 3^{2-1} = 3$.
Inductive Step: For some $n \ge 1$ we assume $a_n \le 3^{2^n-1}$. Now, consider $n+1$. We can write:

$$a_{n+1} = 3a_n^2 \le 3 \times (3^{2^n-1})^2 = 3 \times 3^{2\times(2^n-1)} = 3 \times 3^{2^{n+1}-2} = 3^{2^{n+1}-1}.$$

This is exactly the induction hypothesis for $n+1$.

(c) For every $n \ge 1$, we have $2^n - 1 \le 2^n$ and therefore $3^{2^n-1} \le 3^{2^n}$. This means that our modified hypothesis which we proved in part (b) does indeed imply what we wanted to prove in part (a).

4 Binary Numbers

Note 3

Prove that every positive integer n can be written in binary. In other words, prove that for any positive integer n, we can write

$$n = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0,$$

for some $k \in \mathbb{N}$ and $c_i \in \{0,1\}$ for all $i \le k$.

Solution:

Prove by strong induction on n.

The key insight here is that if n is divisible by 2, then it is easy to get a bit string representation of $(n+1)$ from that of n. However, if n is not divisible by 2, then $(n+1)$ will be, and its binary representation will be more easily derived from that of $(n+1)/2$. More formally:

- Base Case: $n = 1$ can be written as 1×2^0.

- Inductive Step: Assume that the statement is true for all $1 \le m \le n$, where n is arbitrary. Now, we need to consider $n+1$. If $n+1$ is divisible by 2, then we can apply our inductive hypothesis to $(n+1)/2$ and use its representation to express $n+1$ in the desired form.

$$(n+1)/2 = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0$$
$$n+1 = 2 \cdot (n+1)/2 = c_k \cdot 2^{k+1} + c_{k-1} \cdot 2^k + \cdots + c_1 \cdot 2^2 + c_0 \cdot 2^1 + 0 \cdot 2^0.$$

  Otherwise, n must be divisible by 2 and thus have $c_0 = 0$. We can obtain the representation of $n+1$ from n as follows:

$$n = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_1 \cdot 2^1 + 0 \cdot 2^0$$
$$n+1 = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_1 \cdot 2^1 + 1 \cdot 2^0$$

  Therefore, the statement is true.

Here is another alternate solution emulating the algorithm of converting a decimal number to a binary number.

- Base Case: $n = 1$ can be written as 1×2^0.
- Inductive Step: Assume that the statement is true for all $1 \le m \le n$, for arbitrary n. We show that the statement holds for $n+1$. Let 2^m be the largest power of 2 such that $n+1 \ge 2^m$. Thus, $n+1 < 2^{m+1}$. We examine the number $(n+1) - 2^m$. Since $(n+1) - 2^m < n+1$, the inductive hypothesis holds, so we have a binary representation for $(n+1) - 2^m$. (If $(n+1) - 2^m = 0$, then we still have a binary representation, namely $0 \cdot 2^0$.)

  Also, since $n+1 < 2^{m+1}$, $(n+1) - 2^m < 2^m$, so the largest power of 2 in the representation of $(n+1) - 2^m$ is 2^{m-1}. Thus, by the inductive hypothesis,

$$(n+1) - 2^m = c_{m-1} \cdot 2^{m-1} + c_{m-2} \cdot 2^{m-2} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0,$$

  and adding 2^m to both sides gives

$$n+1 = 2^m + c_{m-1} \cdot 2^{m-1} + c_{m-2} \cdot 2^{m-2} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0,$$

  which is a binary representation for $n+1$. Thus, the induction is complete.

Another intuition is that if x has a binary representation, $2x$ and $2x+1$ do as well: shift the bits and possibly place 1 in the last bit. The above induction could then have proceeded from n and used the binary representation of $\lfloor n/2 \rfloor$, shifting and possibly setting the first bit depending on whether n is odd or even.

Note: In proofs using simple induction, we only use $P(n)$ in order to prove $P(n+1)$. Simple induction gets stuck here because in order to prove $P(n+1)$ in the inductive step, we need to assume more than just $P(n)$. This is because it is not immediately clear how to get a representation for $P(n+1)$ using just $P(n)$, particularly in the case that $n+1$ is divisible by 2. As a result, we assume the statement to be true for all of $1, 2, \ldots, n$ in order to prove it for $P(n+1)$.