CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 01B

1 Induction

Prove the following using induction:

(a) Let a and b be integers with $a \neq b$. For all natural numbers $n \geq 1$, $(a^n - b^n)$ is divisible by $(a-b)$.

(b) For all natural numbers n, $(2n)! \leq 2^{2n}(n!)^2$. [Note that 0! is defined to be 1.]

Solution:

(a)
- Base case (n=1): $P(1)$ says that $(a^1 - b^1) = (a-b)$, which is trivially divisible by $(a-b)$.
- Inductive Hypothesis: For arbitrary $n = k \geq 1$, assume that $P(k)$ is true: $a^k - b^k = q_k(a-b), \quad q_k \in \mathbb{Z}$.
- Inductive Step: Prove the statement for $n = k+1$: $P(k+1)$ gives $a^{k+1} - b^{k+1} = q_{k+1}(a-b), \quad q_{k+1} \in \mathbb{Z}$.
  The goal is to express $(a^{k+1} - b^{k+1})$ in terms of $(a^k - b^k)$ and $(a-b)$ (since both of these are divisible by $(a-b)$ which we know their summation is also divisible by $(a-b)$). We can do this as follows:

$$\begin{aligned} a^{k+1} - b^{k+1} &= a(a^k - b^k) + b^k(a-b) \\ &= a \underbrace{(a^k - b^k)}_{\text{divisble by } (a-b)} \qquad \text{(Inductive Hypothesis)} \\ &\quad + b^k(a-b) \end{aligned}$$

Alternatively we can write the following:

$$a^{k+1} - b^{k+1} = \frac{1}{2}[(a+b) \underbrace{(a^k - b^k)}_{\text{divisble by } (a-b)} + (a-b)(a^k + b^k)]$$

again each of the terms in the parentheses is divisible by $(a-b)$. For this argument, one should really also verify that both of those terms are even (so that both are integers when divided by 2); but that's easy to see since the parity of the two terms in the two products is equal.

Thus, $a^{k+1} - b^{k+1} = q_{k+1}(a-b), \quad q_{k+1} \in \mathbb{Z}$.

Hence, $(a^n - b^n)$ is divisble by $(a-b)$ for all $n \geq 1$ by induction.

(b)
- Base case (n=0): $P(0)$ asserts that $(2(0))! = 1 = 2^{(2(0))}(0!)^2$. So we showed the base case is correct.
- Inductive Hypothesis: For arbitrary $n = k \geq 0$, assume that $P(k)$ is correct which leads to $(2k)! \leq 2^{2k}(k!)^2$.
- Inductive Step: Prove the statement for $n = k+1$: i.e., prove that $(2(k+1))! \leq 2^{2(k+1)}((k+1)!)^2$.

$$\begin{aligned}
(2(k+1))! &= (2k)!(2k+2)(2k+1) \\
&\leq 2^{2k}(k!)^2 2(k+1)(2k+1) \qquad \text{(Inductive Hypothesis)} \\
&= 2^{2k+1}(k+1)!k!(2k+1) \\
&\leq 2^{2k+1}(k+1)!k!(2k+2) \\
&\leq 2^{2(k+1)}(k+1)!(k+1)! \\
&= 2^{2(k+1)}((k+1)!)^2.
\end{aligned}$$

Thus, $(2(k+1))! \leq 2^{2(k+1)}((k+1)!)^2$.
Hence, $(2n)! \leq 2^{2n}(n!)^2$ holds for all $n \geq 0$ by induction.

2 Make It Stronger

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 induction hypothesis be simply $a_n \leq 3^{2^n}$? Show why this does not work.

(b) Try to instead prove the statement $a_n \leq 3^{2^n-1}$ using induction. Does this statement imply what you tried to prove in the previous part?

Solution:

(a) Try to prove that for every $n \geq 1$, we have $a_n \leq 3^{2^n}$ by induction.

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

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

However, what we wanted was to get an inequality of the form: $a_{n+1} \leq 3^{2^{n+1}}$. 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 $a_1 = 1 \leq 3^{2-1} = 3$.
Inductive Step: For some $n \geq 1$ we assume $a_n \leq 3^{2^n-1}$. Now, consider $n+1$. We can write:

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

This is exactly the induction hypothesis for $n+1$. Note that for every $n \geq 1$, we have $2^n - 1 \leq 2^n$ and therefore $3^{2^n-1} \leq 3^{2^n}$. This means that our modified hypothesis which we proved here does indeed imply what we wanted to prove in the previous part. This is called "strengthening" the induction hypothesis because we proved a stronger statement and by proving that statement to be true, we proved our original statement to be true as well.

3 Binary Numbers

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

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

where $k \in \mathbb{N}$ and $c_k \in \{0, 1\}$.

Solution:

Prove by strong induction on n. (Note that this is the first discussion where the students use strong induction, so it is important that this problem be done in an interactive way that shows them how simple induction gets stuck.)

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 $1 \leq m \leq n$, 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.

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 $P(n+1)$.