Chapter 1

Induction and Asymptotic Notations.

1.1 Induction.

What is induction?

1. A mathematical proof technique. It is essentially used to prove that a property $P(n)$ holds for every natural number n.

2. The method of induction requires two cases to be proved:

   (a) The first case, called the base case, proves that the property holds for the first element.

   (b) The second case, called the induction step, proves that if the property holds for one natural number, then it holds for the next natural number.

3. The domino metaphor.

The two types of induction, their steps, and why it makes sense (Strong vs Weak) - Emphasize the change in the induction step.

Example 1. (Weak induction) Prove that $\forall n \in N \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Proof. Base: For $n = 1$, $\sum_{i=0}^{1} 1 = 1 = \frac{(1+1)\cdot 1}{2}$.

Assumption: Assume that the claim holds for n. Step:

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

Example 2. (Weak induction) Let $q \in \mathbb{R}/\{1\}$, consider the geometric series $1, q, q^2, q^3 .... q^k ....$ Prove that the sum of the first k elements is

$$1 + q + q^2 + ... + q^{k-1} + q^k = \frac{q^{k+1} - 1}{q - 1}$$

Proof. Base: For $n = 1$, we get $\frac{q^{k+1}-1}{q-1} = \frac{q-1}{q-1} = 1$. Assumption: Assume that the claim holds for k. then: Step:

$$1 + q + q^2 + ... + q^{k-1} + q^k + q^{k+1} = \frac{q^k - 1}{q - 1} + q^{k+1} = \frac{q^{k+1} - 1 + q^{k+1}(q - 1)}{q - 1} = \frac{q^{k+1} - 1 + q^{k+2} - q^{k+1}}{q - 1} = \frac{q^{k+2} - 1}{q - 1}$$

Example 3. (Strong induction) Let there be a chocolate bar that consists of n square chocolate blocks. Then it takes exactly $n - 1$ snaps to separate it into the n squares no matter how we split it.

Proof. By strong induction. Base: For $n = 1$, it is clear that we need 0 snaps. Assumption: Assume that for **every** $m < n$, this claim holds.

Step: We have in our hand the given chocolate bar with n square chocolate blocks. Then we may snap it anywhere we like, to get two new chocolate bars: one with some $k \in [n]$ chocolate blocks and one with $n - k$ chocolate blocks. From the induction assumption, we know that it takes $k - 1$ snaps to separate the first bar, and $n - k - 1$ snaps for the second one. And to sum them up, we got exactly

$$(k - 1) + (n - k - 1) + 1 = n - 1$$

snaps.

1.2 Asymptotic Notations.

Definition Let $f, g : \mathbb{N} \to \mathbb{R}^+$. We say that $f(n) = O(g(n))$ if $\exists N \in \mathbb{N}, \exists c > 0$ s.t. $\forall n \geq N \ : \ f(n) \leq c \cdot g(n)$

Example For exmaple, if $f(n) = n + 10$ and $g(n) = n^2$, then $f(n) = O(g(n))$ (Draw the graphs) for $n \geq 5$: $f(n) = n + 10 \leq n + 2n = 3n \leq n \cdot n = n^2$

Definition Let $f, g : \mathbb{N} \to \mathbb{R}$ We say that $f(n) = \Omega(g(n))$ if $g(n) = O(f(n))$, equivalently, $\exists N \in \mathbb{N}, \exists c > 0$ s.t. $\forall n \geq N c_0 g(n) \leq f(n)$

Example Also if $f(n) = 5n$ and $g(n) = n^2$, then $f(n) = O(g(n))$ (Now discuss intuition - no matter how much we “stretch” f, g is still the winner)

Definition Let $f, g : \mathbb{N} \to \mathbb{R}$, We say that $f(n) = \Omega(g(n))$ if: $\exists N \in \mathbb{N}, \exists c > 0$ s.t $\forall n \geq N \ f(n) \geq c \cdot g(n)$.

Example For exmaple, if $f(n) = n + 10$ and $g(n) = n^2$, then $g(n) = \Omega(f(n))$

Definition Let $f, g : \mathbb{N} \to \mathbb{R}$, We say that $f(n) = \Theta(g(n))$ if: $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$ That is, we say that $f(n) = \Theta(g(n))$ if: $\exists N \in \mathbb{N}, \exists c_1, c_2 > 0$ s.t. $\forall n \geq N \ c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$

Example For every $f : \mathbb{N} \to \mathbb{R}$, $f(n) = \Theta(f(n))$

Example If $p(n) = n^5$ and $q(n) = 0.5n^5 + n$, then $p(n) = \Theta(q(n))$ But why is this example true? This next Lemma helps for intuition:

Lemma $\lim_{n\to\infty} \frac{f(n)}{g(n)} < \infty \Rightarrow f(n) = O(g(n))$

Proof. Assume that $l = \lim_{n\to\infty} \frac{f(n)}{g(n)} < \infty$. Then for some $N \in \mathbb{N}$ we have that for all $n \geq N$: $\frac{f(n)}{g(n)} < l + 1 \Rightarrow f(n) < (l+1)g(n)$ Which is exactly what we wanted.

1.3 Examples with proofs.

Claim $n = O(2^n)$ (This must seem very silly, but even though we have a strong feeling it's true, we still need to learn how to PROVE it) Proof. We will prove by induction that $\forall n \geq 1$, $2^n \geq n$, and that will suffice. Basis: $n = 1$, so it is clear that: $n = 1 < 2 = 2^n$ Assumption: Assume that $n < 2^n$ for some n. Step: We will prove for $n + 1$. It holds that:

$$n + 1 < 2^n + 1 < 2^n + 2^n = 2^{n+1}$$

Claim Let $p(n)$ be a polynomial of degree d and let $q(n)$ be a polynomial of degree k. Then:

1. $d \leq k \Rightarrow p(n) = O(q(n))$ (set upper bound over the quotient)
2. $d \geq k \Rightarrow p(n) = \Omega(q(n))$ (an exercise)
3. $d = k \Rightarrow p(n) = \Theta(g(n))$ (an exercise)

Proof (Of 1) First, let's write down $p(n), g(n)$ explicitly:

$$p(n) = \sum_{i=0}^{d} \alpha_i n^i,\ g(n) = \sum_{j=0}^{k} \beta_j n^j$$

Now let's manipulate their quotient:

$$\frac{p(n)}{q(n)} = \frac{\sum_{i=0}^{d} \alpha_i n^i}{\sum_{j=0}^{k} \beta_j n^j} = \frac{\sum_{i=0}^{d} \alpha_i n^i}{\sum_{j=0}^{k} \beta_j n^j} \cdot \frac{n^{k-1}}{n^{k-1}} = \frac{\sum_{i=0}^{d} \alpha_i n^{i-k+1}}{\sum_{j=0}^{k} \beta_j n^{j-k+1}} \leq$$

$$\leq \frac{\sum_{i=0}^{d} \alpha_i}{\beta_k} < \infty$$

And now we can use the lemma that we have proved earlier.

1.4 Logarithmic Rules.

Just a quick reminder of logarithmic rules:

1. $log_a x \cdot y = log_a x + log_a y$
2. $log_a \frac{x}{y} = log_a x - log_a y$

3. $log_a x^m = m \cdot log_a x$

4. Change of basis: $\frac{log_a x}{log_a y} = log_y x$

And so we get that:

Remark 1.4.1. *For every $x, a, b \in \mathbb{R}$, we have that $log_a x = \Theta(log_b x)$*

Example. Let $f(n)$ be defined as:

$$f(n) = \begin{cases} f\left(\lfloor \frac{n}{2} \rfloor\right) + 1 & \text{for } n > 1 \\ 5 & \text{else} \end{cases}$$

Let's find an asymptotic upper bound for $f(n)$. let's guess $f(n) = O(\log(n))$.

Proof. We'll prove by strong induction that : $f(n) < c\log(n) - 1$ for $c = 8$ And that will be enough (why? This implies $f(n) = O(\log(n))$). Base: $n = 2$. Clearly, $f(2) = 6 < 8$ Assumption: Assume that for every m ¡ n, this claim holds. Step: Then we get:

$$\begin{aligned} f(n) &= f\left(\lfloor \frac{n}{2} \rfloor\right) + 1 \leq c\log\left(\lfloor \frac{n}{2} \rfloor\right) + 1 \\ &\leq c\log(n) - c\log(2) + 1 \leq c\log(n) \quad \text{for } c = 8 \end{aligned}$$